

Multilevel Polarization of Polar Codes Over Arbitrary Discrete Memoryless Channels

Aria G. Sahebi and S. Sandeep Pradhan

Department of Electrical Engineering and Computer Science,

University of Michigan, Ann Arbor, MI 48109, USA.

Email: ariaghs@umich.edu, pradhanv@umich.edu

Abstract

It is shown that polar codes achieve the symmetric capacity of discrete memoryless channels with arbitrary input alphabet sizes. It is shown that in general, channel polarization happens in several, rather than only two levels so that the synthesized channels are either useless, perfect or “partially perfect”. Any subset of the channel input alphabet which is closed under addition, induces a coset partition of the alphabet through its shifts. For any such partition of the input alphabet, there exists a corresponding partially perfect channel whose outputs uniquely determine the coset to which the channel input belongs. By a slight modification of the encoding and decoding rules, it is shown that perfect transmission of certain information symbols over partially perfect channels is possible. Our result is general regarding both the cardinality and the algebraic structure of the channel input alphabet; i.e we show that for any channel input alphabet size and any Abelian group structure on the alphabet, polar codes are optimal. It is also shown through an example that polar codes when considered as group/coset codes, do not achieve the capacity achievable using coset codes over arbitrary channels.

Index Terms

Polar codes, Channel polarization, Group codes, Discrete memoryless channels

I. INTRODUCTION

Polar codes were originally proposed by Arikan in [1] for discrete memoryless channels with a binary input alphabet. Polar codes over binary input channels are shifted linear (coset) codes capable of achieving

This work was presented in part in the 49th Annual Allerton Conference, Allerton, IL, USA, September 28 - 30, 2011.

This work was supported by NSF grants CCF-0915619 and CCF-1116021.

the symmetric capacity of channels. These codes are constructed based on the Kronecker power of the 2×2 matrix $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and are the first known class of capacity achieving codes with an explicit construction.

It is known that non-binary codes outperform binary codes in certain communication settings. Therefore, constructing capacity achieving codes for channels of arbitrary input alphabet sizes is of great interest. In order to construct capacity achieving codes over non-binary channels, there have been attempts to extend polar coding techniques to channels of arbitrary input alphabet sizes. It is shown in [2] that polar codes achieve the symmetric capacity of channels when the size of the input alphabet is a prime. For channels of arbitrary input alphabet sizes, it is shown in [2] that the original construction of polar codes does not necessarily achieve the symmetric capacity of the channel due to the fact that polarization (into two levels) may not occur for arbitrary channels. In the same paper, a randomized construction of polar codes based on permutations is proposed. In this approach, the existence of a polarizing transformation is shown by a (small) random coding argument over the ensemble of permutations of the input alphabet. In another approach in [2], a code construction method is proposed which is based on the decomposition of the composite input channel into sub-channels of prime input alphabet sizes. In this multilevel code construction method, a separate polar code is designed for each sub-channel of prime input alphabet size. It is shown in [3] that for channels for which the input alphabet size is a prime power, polar codes defined on the input alphabet can achieve the symmetric capacity without the need to use multilevel code construction methods.

Another related work is [4], in which the authors have shown that polar codes are sufficient to achieve the uniform sum rate on any binary input MAC and it is stated that the same technique can be used for the point-to-point problem to achieve the symmetric capacity of the channel when the size of the alphabet is a power of 2. In a recent work, it has been shown in [5] that polar codes achieve the capacity of channels with input alphabet size a power of 2.

In this paper, we show that with a slight modification of the encoding and decoding rules, standard polar codes are sufficient to achieve the symmetric capacity of all discrete memoryless channels. Our result is general regarding both the cardinality and the algebraic structure of the channel input alphabet; i.e we show that for any channel input alphabet size and any Abelian group structure on the alphabet, polar codes are optimal. This result was first reported in [6]. We use a combination of algebraic and

coding techniques and show that in general, channel polarization occurs in several levels rather than only two: Suppose the channel input alphabet is \mathbf{G} and is endowed with an Abelian group structure. Then for any subset H of the channel input alphabet \mathbf{G} which is closed under addition (i.e any subgroup of \mathbf{G}), there may exist a corresponding polarized channel which can perfectly transmit the index of the shift (coset) of H in \mathbf{G} which contains the input. As an example, for a channel of input \mathbb{Z}_6 , there are four subgroups of the input alphabet: **i)** $\{0\}$ with cosets $\{0\}, \{1\}, \{2\}, \{3\}, \{4\}$ and $\{5\}$, **ii)** $\{0, 3\}$ with cosets $\{0, 3\}, \{1, 4\}$ and $\{2, 5\}$, **iii)** $\{0, 2, 4\}$ with cosets $\{0, 2, 4\}$ and $\{1, 3, 5\}$ and **iv)** \mathbb{Z}_6 . For polar codes over \mathbb{Z}_6 , the asymptotic synthesized channels can exist in four forms: **i)** can determine which one of the cosets $\{0\}, \{1\}, \{2\}, \{3\}, \{4\}$ or $\{5\}$ contains the input symbol, (perfect channels with capacity $\log_2 6$ bits per channel use), **ii)** can determine which one of the cosets $\{0, 3\}, \{1, 4\}$ or $\{2, 5\}$ contains the input symbol (partially perfect channels with capacity $\log_2 3$ bits per channel use), **iii)** can determine which one of the cosets $\{0, 2, 4\}$ or $\{1, 3, 5\}$ contains the input symbol (partially perfect channels with capacity 1 bit per channel use), **iv)** can only determine the input belongs to $\{0, 1, 2, 3, 4, 5\}$ (useless channel). Cases **i,ii,iii** and **iv** correspond to coset decompositions of \mathbb{Z}_6 based on subgroups $\{0\}, \{0, 3\}, \{0, 2, 4\}$ and $\{0, 1, 2, 3, 4, 5\}$ respectively.

Although standard binary polar codes are group (linear) codes, the class of capacity achieving codes constructed and analyzed in this paper are not group codes. It is known that group codes do not generally achieve the symmetric capacity of discrete memoryless channels [7]. Hence, one could have predicted that standard polar codes cannot achieve the symmetric capacity of arbitrary channels and a modification of the encoding rule is indeed necessary to achieve that goal. Due to the modifications we make to the encoding rule of polar codes, the constructed codes fall into a larger class of structured codes called nested group codes.

The paper is organized as follows: In Section II, some definitions and basic facts are stated which are used in the paper. In Section III, we present two motivating examples of 4-ary and 6-ary channels and observe the polarization effect on these channels. In Section IV, we show that polar codes achieve the symmetric capacity of channels with input alphabet size $q = p^r$ where p is a prime and r is an integer. This result is generalized to arbitrary channels in Section V. In Section VI, the relation of polar codes to group codes is discussed and two examples of channels over \mathbb{Z}_4 are provided. In the first example, we show that polar codes approach the capacity of channels achievable using group codes. The intent of the second example is to show that this is not generally the case; i.e. polar codes do not generally approach

the capacity of channels achievable using group/coset codes.

II. PRELIMINARIES

1) *Source and Channel Models:* We consider discrete memoryless and stationary channels used without feedback. We associate two finite sets \mathcal{X} and \mathcal{Y} with the channel as the channel input and output alphabets. These channels can be characterized by a conditional probability law $W(y|x)$ for $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. The channel is specified by $(\mathcal{X}, \mathcal{Y}, W)$. The source of information generates messages over the set $\{1, 2, \dots, M\}$ uniformly for some positive integer M .

2) *Achievability and Capacity:* A transmission system with parameters (n, M, τ) for reliable communication over a given channel $(\mathcal{X}, \mathcal{Y}, W)$ consists of an encoding mapping $e : \{1, 2, \dots, M\} \rightarrow \mathcal{X}^n$ and a decoding mapping $d : \mathcal{Y}^n \rightarrow \{1, 2, \dots, M\}$ such that

$$\frac{1}{M} \sum_{m=1}^M W^n(d(Y^n) \neq m | X^n = e(m)) \leq \tau$$

Given a channel $(\mathcal{X}, \mathcal{Y}, W)$, the rate R is said to be achievable if for all $\epsilon > 0$ and for all sufficiently large n , there exists a transmission system for reliable communication with parameters (n, M, τ) such that

$$\frac{1}{n} \log M \geq R - \epsilon, \quad \tau \leq \epsilon$$

3) *Symmetric Capacity and the Bhattacharyya Parameter:* For a channel $(\mathcal{X}, \mathcal{Y}, W)$, the symmetric capacity is defined as $I^0(W) = I(X; Y)$ where the channel input X is uniformly distributed over \mathcal{X} and Y is the output of the channel; i.e. for $q = |\mathcal{X}|$,

$$I^0(W) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \frac{1}{q} W(y|x) \log \frac{W(y|x)}{\sum_{\tilde{x} \in \mathcal{X}} \frac{1}{q} W(y|\tilde{x})}$$

The Bhattacharyya distance between two distinct input symbols x and \tilde{x} is defined as

$$Z(W_{\{x, \tilde{x}\}}) = \sum_{y \in \mathcal{Y}} \sqrt{W(y|x)W(y|\tilde{x})}$$

and the average Bhattacharyya distance is defined as

$$Z(W) = \sum_{\substack{x, \tilde{x} \in \mathcal{X} \\ x \neq \tilde{x}}} \frac{1}{q(q-1)} Z(W_{\{x, \tilde{x}\}})$$

4) *Binary Polar Codes*: For any $N = 2^n$, a polar code of length N designed for the channel $(\mathbb{Z}_2, \mathcal{Y}, W)$ is a linear code characterized by a generator matrix G_N and a set of indices $A \subseteq \{1, \dots, N\}$ of *perfect channels*. The generator matrix for polar codes is defined as $G_N = B_N F^{\otimes n}$ where B_N is a permutation of rows, $F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and \otimes denotes the Kronecker product. The set A is a function of the channel. The decoding algorithm for polar codes is a specific form of successive cancellation [1].

5) *Groups, Rings and Fields*: All groups referred to in this paper are *Abelian groups*. Given a group $(\mathbf{G}, +)$, a subset H of \mathbf{G} is called a *subgroup* of \mathbf{G} if it is closed under the group operation. In this case, $(H, +)$ is a group on its own right. This is denoted by $H \leq \mathbf{G}$. A *coset* C of a subgroup H is a shift of H by an arbitrary element $a \in \mathbf{G}$ (i.e. $C = a + H$ for some $a \in \mathbf{G}$). For any subgroup H of \mathbf{G} , its cosets partition the group \mathbf{G} . A *transversal* T of a subgroup H of \mathbf{G} is a subset of \mathbf{G} containing one and only one element from each coset (shift) of H .

We give some examples in the following: The simplest non-trivial example of groups is \mathbb{Z}_2 with addition mod-2 which is a *ring* and a *field* with multiplication mod-2. The group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is also a ring and a field under component-wise mod-2 addition and a carefully defined multiplication. The group \mathbb{Z}_4 with mod-4 addition and multiplication is a ring but not a field since the element $2 \in \mathbb{Z}_4$ does not have a multiplicative inverse. The subset $\{0, 2\}$ is a subgroup of \mathbb{Z}_4 since it is closed under mod-4 addition. $\{0\}$ and \mathbb{Z}_4 are the two other subgroups of \mathbb{Z}_4 . The group \mathbb{Z}_6 is neither a field nor a ring. Subgroups of \mathbb{Z}_6 are: $\{0\}$, $\{0, 3\}$, $\{0, 2, 4\}$ and \mathbb{Z}_6 .

6) *Polar Codes Over Abelian Groups*: For any discrete memoryless channel, there always exists an Abelian group of the same size as that of the channel input alphabet. In general, for an Abelian group, there may not exist a multiplication operation. Since polar encoders are characterized by a matrix multiplication, before using these codes for channels of arbitrary input alphabet sizes, a generator matrix for codes over Abelian groups needs to be properly defined. In Appendix A, a convention is introduced to generate codes over groups using $\{0, 1\}$ -valued generator matrices.

7) *Group Codes:* Let the channel input alphabet \mathcal{X} be equipped with the structure of a finite Abelian group \mathbf{G} of the same size. Then the channel is specified by $(\mathbf{G}, \mathcal{Y}, W)$. A group code over \mathbf{G} of length N for this channel is any subgroup of \mathbf{G}^N . The group capacity of a channel $(\mathbf{G}, \mathcal{Y}, W)$ is the maximum achievable rate using group codes over \mathbf{G} for this channel. Group codes generalize the notion of linear codes over fields to channels with composite input alphabet sizes. A coset code is a shift of a group code by a constant vector.

8) *Notation:* We denote by $O(\epsilon)$ any function of ϵ which is right-continuous around 0 and that $O(\epsilon) \rightarrow 0$ as $\epsilon \downarrow 0$. We denote by $a \approx_\epsilon b$ to mean $a = b + O(\epsilon)$.

For positive integers N and r , let $\{A_0, A_1, \dots, A_r\}$ be a partition of the index set $\{1, 2, \dots, N\}$. Given sets T_t for $t = 0, \dots, r$, the direct sum $\bigoplus_{t=0}^r T_t^{A_t}$ is defined as the set of all tuples $u_1^N = (u_1, \dots, u_N)$ such that $u_i \in T_t$ whenever $i \in A_t$.

III. MOTIVATING EXAMPLES

A key property of the basic polarizing transforms used for binary polar codes is that they have perfect and useless channels as their “fixed points”; in the sense that, if these transforms are applied to a perfect (useless) channel, the resulting channel is also perfect (useless). In the following, we try to demonstrate that for non-binary channels, the basic transforms have fixed points which are neither perfect nor useless. Consider a 4-ary channel $(\mathbb{Z}_4, \mathcal{Y}, W)$ and assume the channel is such that $W(y|u) = W(y|u+2)$ for all $y \in \mathcal{Y}$ and all $u \in \mathbb{Z}_4$; i.e. the channel cannot distinguish between inputs u and $u+2$. Consider the transformed channels W^- and W^+ originally introduced in [1] (Refer to Equations (5) and (6) of the current paper). It turns out that

$$\begin{aligned} W^+(y_1, y_2, u_1|u_2) &= W^+(y_1, y_2, u_1|u_2+2) \\ W^-(y_1, y_2|u_1) &= W^-(y_1, y_2|u_1+2) \end{aligned}$$

for all $y_1, y_2 \in \mathcal{Y}$ and all $u_1, u_2 \in \mathbb{Z}_4$. This observation is closely related to the fact that $\{0, 2\}$ is closed under addition mod-4; i.e. the fact that $\{0, 2\}$ forms a subgroup of \mathbb{Z}_4 . This means that the transformed channels inherit this characteristic feature of the original channel, in the sense that they cannot distinguish between inputs u_i and u_i+2 ($i = 2$ for W^+ and $i = 1$ for W^-). This suggests that even in the asymptotic regime, the transformed channels can only distinguish between the sets $\{0, 2\}$ and $\{1, 3\}$, and not within

each set. In the following, we give an example for which such cases indeed exist in the asymptotic regime.

Consider the channel depicted in Figure 1. For this channel, the symmetric capacity is equal to $C = I(X; Y) = 2 - \epsilon - 2\lambda$. Depending on the values of the parameters ϵ and λ , this channel can present three extreme cases: 1) If $\lambda = 1$, this channel is useless. 2) If $\epsilon = 1$, this channel cannot distinguish between inputs u and $u + 2$ and has a capacity of 1 bit per channel use. 3) If $\epsilon = \lambda = 0$, this channel is perfect and has a capacity of 2 bits per channel use.

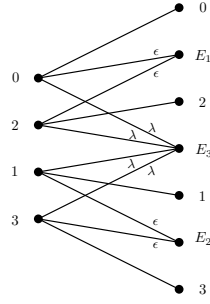


Fig. 1: Channel 1: The input of the channel has the structure of the group \mathbb{Z}_4 . The parameters ϵ and λ take values from $[0, 1]$ such that $\epsilon + \lambda \leq 1$. E_1 and E_2 are erasures connected to cosets of the subgroup $\{0, 2\}$. The lines connecting the output symbols 0, 2, 1, 3 to their corresponding inputs, represent a conditional probability of $1 - \epsilon - \lambda$. For this channel, the process $I(W^{b_1 b_2 \dots b_n})$ can be explicitly found for each n and the multilevel polarization can be observed.

Given a sequence of bits $b_1 b_2 \dots b_n$, define $W^{b_1 b_2 \dots b_n}$ as in [1, Section IV], and let $I(W^{b_1 b_2 \dots b_n})$ be the mutual information between the input and output of $W^{b_1 b_2 \dots b_n}$ when the input is uniformly distributed. We can find $I(W^{b_1 b_2 \dots b_n})$ using the following recursion for which the proof can be found in Appendix B.

Define $\epsilon_0 = \epsilon$ and $\lambda_0 = \lambda$. For $i = 1, \dots, n$,

- If $b_i = 1$, let

$$\begin{cases} \epsilon_i = \epsilon_{i-1}^2 + 2\epsilon_{i-1}\lambda_{i-1} \\ \lambda_i = \lambda_{i-1}^2 \end{cases} \quad (1)$$

- If $b_i = 0$, let

$$\begin{cases} \epsilon_i = 2\epsilon_{i-1} - (\epsilon_{i-1}^2 + 2\epsilon_{i-1}\lambda_{i-1}) \\ \lambda_i = 2\lambda_{i-1} - \lambda_{i-1}^2 \end{cases} \quad (2)$$

Then we have $I(W^{b_1 b_2 \dots b_n}) = 2 - \epsilon_n - 2\lambda_n$.

Consider the function $f : [0, 1]^2 \rightarrow [0, 1]^2$, $f(\epsilon, \lambda) = (\epsilon^2 + 2\epsilon\lambda, \lambda^2)$ corresponding to Equation (1). The fixed points of this function are given by $(0, 1)$, $(1, 0)$ and $(0, 0)$. Similarly, consider the function $g : [0, 1]^2 \rightarrow [0, 1]^2$, $g(\epsilon, \lambda) = (2\epsilon - (\epsilon^2 + 2\epsilon\lambda), 2\lambda - \lambda^2)$ corresponding to Equation (2). It turns out that the fixed points of g are the same as those of f . This suggests that in the limit, the transformed channels converge to one of three extreme cases discussed above. Figures 2 and 3 show that it is indeed the case and depicts the three level polarization of the mutual information process $I(W^{b_1 b_2 \dots b_n})$ to a discrete random variable I^∞ as n grows.

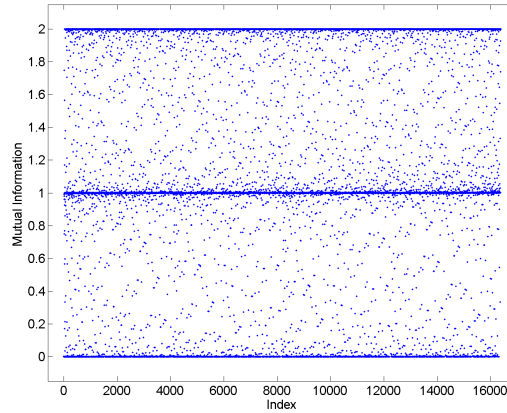


Fig. 2: The behavior of $I(W^{b_1 b_2 \dots b_n})$ for $n = 14$ for Channel 1 when $\epsilon = 0.4$ and $\lambda = 0.2$. The three solid lines represent the three discrete values of I^∞ with positive probability.

When $N = 2^n$ is large, let N_0 be the number of useless channels (corresponding to the width of the first step in Figure 3), N_1 be the number of partially perfect channels (corresponding to the width of the second step in Figure 3) and N_2 be the number of perfect channels (corresponding to the width of the third step in Figure 3). Since the mutual information process is a martingale, it follows that

$$C = \mathbb{E}\{I^\infty\} \approx \frac{N_0}{N} \times 0 + \frac{N_1}{N} \times 1 + \frac{N_2}{N} \times 2$$

where C is the symmetric capacity of the channel. Consider the following encoding rule: For indices corresponding to useless channels, let the input symbol take values from $\{0\}$ (from the transversal of the subgroup \mathbb{Z}_4 of \mathbb{Z}_4 i.e. fix the input). For indices corresponding to partially perfect channels, let the input symbol take values from $\{0, 1\}$ (from the transversal of the subgroup $\{0, 2\}$ of \mathbb{Z}_4). For indices corresponding to perfect channels, let the input symbol take values from \mathbb{Z}_4 (choose information

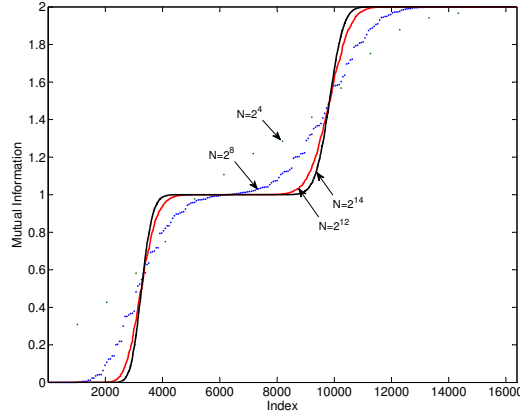


Fig. 3: The asymptotic behavior of $I(W^{b_1 b_2 \dots b_n})$, $N = 2^n = 2^4, 2^8, 2^{12}, 2^{14}$ for Channel 1 when the data is sorted. We observe that for this channel, all three extreme cases appear with positive probability. In general, it is possible to have fewer cases in the asymptotic regime.

symbols from the transversal of the subgroup $\{0\}$ of \mathbb{Z}_4). It turns out that this encoding rule used with an appropriate decoding rule has a vanishingly small probability of error as N becomes large. The rate of this code is equal to

$$R = \frac{1}{N} (N_0 \log_2 1 + N_1 \log_2 2 + N_2 \log_2 4)$$

This means $R = C$ is achievable using polar codes.

Next, we consider a channel with a composite input alphabet size. Consider the channel depicted in Figure 4. We call this Channel 2. It turns out that given a sequence of bits $b_1 b_2 \dots b_n$, the transformed channel $W^{b_1 b_2 \dots b_n}$ is (equivalent to) a channel of the same type as Channel 2 but with possibly different parameters ϵ, λ and γ . At each step n , the corresponding parameters can be found using the following recursion: Define $\epsilon_0 = \epsilon$, $\lambda_0 = \lambda$ and $\gamma_0 = \gamma$. For $i = 1, \dots, n$,

- If $b_i = 1$, let

$$\begin{cases} \gamma_i = \gamma_{i-1}^2 + 2\gamma_{i-1}\lambda_{i-1} \\ \epsilon_i = \epsilon_{i-1}^2 + 2\epsilon_{i-1}\lambda_{i-1} \\ \lambda_i = \lambda_{i-1}^2 \end{cases} \quad (3)$$

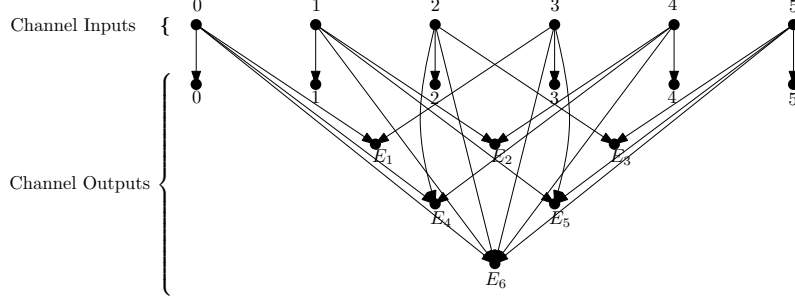


Fig. 4: Channel 2: A channel with a composite input alphabet size. For this channel, the process I^n can be explicitly found for each n and the multilevel polarization can be observed. E_1 , E_2 and E_3 are erasures corresponding to cosets of the subgroup $\{0, 3\}$ and E_4 and E_5 are erasures corresponding to cosets of the subgroup $\{0, 2, 4\}$. The lines connected to outputs E_1, E_2 and E_3 correspond to a conditional probability of γ , the lines connected to outputs E_4 and E_5 correspond to a conditional probability of ϵ , the lines connected to the output E_6 correspond to a conditional probability of λ , and the lines connected to outputs 0, 1, 2, 3, 4 and 5 correspond to a conditional probability of $1 - \gamma - \epsilon - \lambda$. The parameters $\gamma, \epsilon, \lambda$ take values from $[0, 1]$ such that $\gamma + \epsilon + \lambda \leq 1$.

- If $b_i = 0$, let

$$\begin{cases} \gamma_i = 2\gamma_{i-1} - (\gamma_{i-1}^2 + 2\gamma_{i-1}\lambda_{i-1}) \\ \epsilon_i = 2\epsilon_{i-1} - (\epsilon_{i-1}^2 + 2\epsilon_{i-1}\lambda_{i-1}) \\ \lambda_i = 2\lambda_{i-1} - (\lambda_{i-1}^2) \end{cases} \quad (4)$$

Then we have

$$I(W^{b_1 b_2 \dots b_n}) = \log_2 6 - \gamma_n \log_2 2 - \epsilon_n \log_2 3 - \lambda_n \log_2 6$$

The proof of the recursion formulas for Channel 2 is similar to that of Channel 1 and is omitted. The fixed points of the functions corresponding to Equations (3) and (4) are given by $(0, 0, 0)$, $(1, 0, 0)$, $(0, 1, 0)$, $(1, 1, 0)$, $(0, 0, 1)$, $(-1, 0, 1)$, $(0, -1, 1)$ and $(-1, -1, 1)$, out of which $(0, 0, 0)$, $(1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$ are admissible. Note that $(0, 0, 0)$ corresponds to a perfect channel with a capacity of $\log_2 6$ bits per channel use, $(1, 0, 0)$ corresponds to a partially perfect channel which can perfectly send the index of the coset of the subgroup $\{0, 3\}$ to which the input belongs and has a capacity of $\log_2 3$ bits per channel use, $(0, 1, 0)$ corresponds to a partially perfect channel which can perfectly send the index of the coset of the subgroup $\{0, 2, 4\}$ to which the input belongs and has a capacity of $\log_2 2$ bits per channel use, and $(0, 0, 1)$ corresponds to a useless channel. This suggests that in the limit, the transformed channels converge to one of these four extreme cases. This can be confirmed using the recursion formulas for this

channel as depicted in Figures 5 and 6. With encoding and decoding rules similar to those of Channel 1, we can show that polar codes achieve the symmetric capacity of this channel.

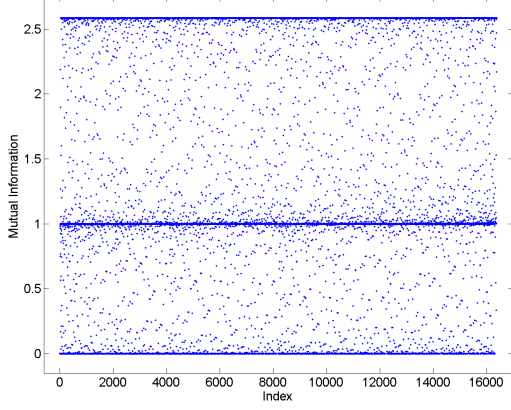


Fig. 5: Polarization of Channel 2 with parameters $\gamma = 0, \epsilon = 0.4, \lambda = 0.2$. The middle line represents the subgroup $\{0, 2, 4\}$ of \mathbb{Z}_6 .

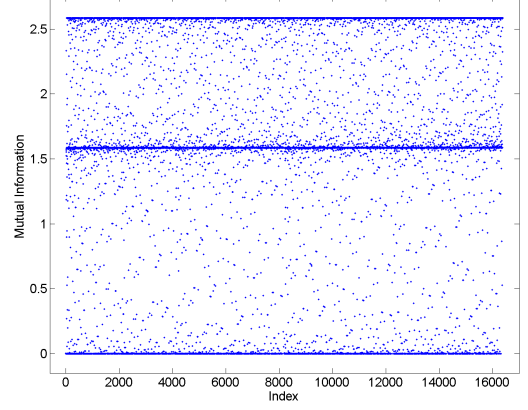


Fig. 6: Polarization of Channel 2 with parameters $\gamma = 0.4, \epsilon = 0, \lambda = 0.2$. The middle line represents the subgroup $\{0, 3\}$ of \mathbb{Z}_6 .

In the next section, we show that polar codes achieve the symmetric capacity of channels with input alphabet size equal to a power of a prime.

IV. POLAR CODES OVER CHANNELS WITH INPUT \mathbb{Z}_{p^r}

In this section, we consider channels of input alphabet size $q = p^r$ for some prime number p and a positive integer r . In this case, the input alphabet of the channel can be considered as a ring with addition and multiplication modulo p^r . We prove the achievability of the symmetric capacity of these channels using polar codes and later in Section V we will generalize this result to channels of arbitrary input alphabet sizes and arbitrary group operations. We note that $O(\epsilon)$ functions used in this paper do not depend on the size of the channel output alphabet.

A. \mathbb{Z}_{p^r} Rings

Let $\mathbf{G} = \mathbb{Z}_{p^r} = \{0, 1, 2, \dots, p^r - 1\}$ with addition and multiplication modulo p^r be the input alphabet of the channel, where p is a prime and r is an integer. For $t = 0, 1, \dots, r$, define the subgroups H_t of \mathbf{G} as the set:

$$H_t = p^t \mathbf{G} = \{0, p^t, 2p^t, \dots, (p^{r-t} - 1)p^t\}$$

and for $t = 0, 1, \dots, r$, define the subsets K_t of \mathbf{G} as $K_t = H_t \setminus H_{t+1}$; i.e. K_t is defined as the set of elements of \mathbf{G} which are a multiple of p^t but are not a multiple of p^{t+1} . Note that K_0 is the set of all invertible elements of \mathbf{G} and $K_r = \{0\}$. One can sort the sets $K_0 > K_1 > \dots > K_r$ in a decreasing order of “invertibility” of its elements. Let T_t be a transversal of H_t in \mathbf{G} ; i.e. a subset of \mathbf{G} containing one and only one element from each coset of H_t in \mathbf{G} . One valid choice for T_t is $\{0, 1, \dots, p^t - 1\}$. Note that given H_t and T_t , each element g of \mathbf{G} can be represented uniquely as a sum $g = \hat{g} + \tilde{g}$ where $\hat{g} \in T_t$ and $\tilde{g} \in H_t$.

B. Recursive Channel Transformation

1) *The Basic Channel Transforms:* It has been shown in [1] that the error probability of polar codes over binary input channels is upper bounded by the sum of Bhattacharyya parameters of certain channels defined by a recursive channel transformation. The same set of synthesized channels appear for polar codes over channels with arbitrary input alphabet sizes. The channel transformations are given by:

$$W^-(y_1, y_2 | u_1) = \sum_{u'_2 \in \mathbf{G}} \frac{1}{q} W(y_1 | u_1 + u'_2) W(y_2 | u'_2) \quad (5)$$

$$W^+(y_1, y_2, u_1 | u_2) = \frac{1}{q} W(y_1 | u_1 + u_2) W(y_2 | u_2) \quad (6)$$

for $y_1, y_2 \in \mathcal{Y}$ and $u_1, u_2 \in \mathbf{G}$. Repeating these operations n times recursively, we obtain $N = 2^n$ channels $W_N^{(1)}, \dots, W_N^{(N)}$. For $i = 1, \dots, N$, these channels are given by:

$$W_N^{(i)}(y_1^N, u_1^{i-1} | u_i) = \sum_{u_{i+1}^N \in \mathbf{G}^{N-i}} \frac{1}{q^{N-i}} W^N(y_1^N | u_1^N G_N)$$

where G_N is the generator matrix for polar codes.

For the case of binary input channels, it has been shown in [1] that as $N \rightarrow \infty$, these channels polarize in the sense that their Bhattacharyya parameters gets either close to zero (perfect channels) or close to one (useless channels). In the next part, we show that in general, when the input alphabet is a prime power, polarization happens in multiple levels so that as $N \rightarrow \infty$ channels get useless, perfect or “partially perfect”.

For an integer n , let J_n be a uniform random variable over the set $\{1, 2, \dots, N = 2^n\}$ and define the random variable $I^n(W)$ as

$$I^n(W) = I(X; Y) \quad (7)$$

where X and Y are the input and output of $W_N^{(J_n)}$ respectively and X is uniformly distributed. It has been shown in [2] that the process I^0, I^1, I^2, \dots is a martingale; hence $\mathbb{E}\{I^n\} = I^0$. For an integer n

and for $d \in \mathbf{G}$, define the random variable $Z_d^n(W) = Z_d(W_N^{(J_n)})$ where for a channel $(\mathbf{G}, \mathcal{Y}, W)$,

$$Z_d(W) = \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} \sqrt{W(y|x)W(y|x+d)} = \frac{1}{q} \sum_{x \in \mathbf{G}} Z(W_{\{x, x+d\}}) \quad (8)$$

This quantity has been defined in [2]. Other than the processes $I^n(W)$ and $Z_d^n(W)$, in the proof of polarization, we need another set of processes $I_H^n(W)$ for $H \leq \mathbf{G}$ which we define in the following. Let H be an arbitrary subgroup of \mathbf{G} . Note that any uniform random variable defined over \mathbf{G} can be decomposed into two uniform and independent random variables \hat{X} and \tilde{X} where \hat{X} takes values from the transversal T of H and \tilde{X} takes values from H . For an integer n , define the random variable $I_H^n(W)$ as

$$I_H^n(W) = I(X; Y | \hat{X}) = I(\tilde{X}; Y | \hat{X}) \quad (9)$$

where X and Y are the input and output of $W_N^{(J_n)}$ respectively. Next lemma shows that $I_H^n(W)$ is a super-martingale.

Lemma IV.1. *For an arbitrary group \mathbf{G} and for any subgroup H of \mathbf{G} , the random process $I_H^n(W)$ defined above is a super-martingale.*

Proof: Define the channels W^- and W^+ as in (5) and (6). Define the random variables U_1, U_2, X_1, X_2, Y_1 and Y_2 where U_1 and U_2 are uniformly distributed over \mathbf{G} , $X_1 = U_1 + U_2$ where addition is the group operation, $X_2 = U_2$ and Y_1 (respectively Y_2) is the channel output when the input is X_1 (respectively X_2). Decompose the random variable U_1 into two uniform and independent random variables \hat{U}_1 and \tilde{U}_1 where \hat{U}_1 takes values from the transversal T of H and \tilde{U}_1 takes values from H . Similarly define, $\hat{U}_2, \hat{X}_1, \hat{X}_2$ and $\tilde{U}_2, \tilde{X}_1, \tilde{X}_2$. We need to show that

$$I(\tilde{U}_1; Y_1 Y_2 | \hat{U}_1) + I(\tilde{U}_2; Y_1 Y_2 U_1 | \hat{U}_2) \leq 2I(\tilde{X}_1; Y_1 | \hat{X}_1)$$

Note that since I^n is a martingale and $I(\tilde{X}_1; Y_1 | \hat{X}_1) = I(X_1; Y_1) - I(\hat{X}_1; Y_1)$, it suffices to show

$$I(\hat{U}_1; Y_1 Y_2) + I(\hat{U}_2; Y_1 Y_2 U_1) \geq 2I(\hat{X}_1; Y_1)$$

We have

$$\begin{aligned} I(\hat{U}_2; Y_1 Y_2 U_1) &= I(\hat{U}_2; Y_1 Y_2 \hat{U}_1 \tilde{U}_1) \\ &= I(\hat{U}_2; Y_1 Y_2 \hat{U}_1) + I(\hat{U}_2; \tilde{U}_1 | Y_1 Y_2 \hat{U}_1) \\ &\geq I(\hat{U}_2; Y_1 Y_2 \hat{U}_1) \end{aligned}$$

Hence,

$$\begin{aligned}
I(\hat{U}_1; Y_1 Y_2) + I(\hat{U}_2; Y_1 Y_2 U_1) &\geq I(\hat{U}_1; Y_1 Y_2) + I(\hat{U}_2; Y_1 Y_2 \hat{U}_1) \\
&= I(\hat{U}_1 \hat{U}_2; Y_1 Y_2) \\
&\stackrel{(a)}{=} I(\hat{X}_1 \hat{X}_2; Y_1 Y_2) = 2I(\hat{X}_1; Y_1)
\end{aligned}$$

where (a) follows since \hat{U}_1 and \hat{U}_2 are recoverable from \hat{X}_1 and \hat{X}_2 . To see this, let U'_1 and U'_2 take values from \mathbf{G} and let $X'_1 = U'_1 + U'_2$ and $X'_2 = U'_2$. We need to show that if X'_1 is in the same coset of H as X_1 (i.e. if $X'_1 - X_1 \in H$ or equivalently $\hat{X}'_1 = \hat{X}_1$) and X'_2 is in the same coset of H as X_2 (i.e. if $X'_2 - X_2 \in H$ or equivalently $\hat{X}'_2 = \hat{X}_2$), then U'_1 is in the same coset of H as U_1 (i.e. $U'_1 - U_1 \in H$ or equivalently $\hat{U}'_1 = \hat{U}_1$) and U'_2 is in the same coset of H as U_2 (i.e. $U'_2 - U_2 \in H$ or equivalently $\hat{U}'_2 = \hat{U}_2$). Note that $X'_2 - X_2 \in H$ implies $U'_2 - U_2 \in H$ and $X'_1 - X_1 \in H$ implies $U'_1 + U'_2 - U_1 - U_2 \in H$. Since $U'_2 - U_2 \in H$ (and hence $U_2 - U'_2 \in H$), it follows that $U'_1 - U_1 \in H + U_2 - U'_2 = H$. This concludes the lemma. \blacksquare

2) *Asymptotic Behavior of Synthesized Channels:* We restate Lemma 2 of [2] with a slight generalization:

Lemma IV.2. Suppose B_n , $n \in \mathbb{Z}^+$ is a $\{-, +\}$ -valued process with $P(B_n = -) = P(B_n = +) = \frac{1}{2}$. Suppose I_n and T_n are two processes adapted to the process B_n satisfying the following conditions

- 1) I_n takes values in the interval $[0, 1]$.
- 2) I_n converges almost surely to a random variable I_∞ .
- 3) T_n takes values in the interval $[0, 1]$.
- 4) $T_{n+1} = T_n^2$ when $B_{n+1} = +$.
- 5) If $T_n < \epsilon$ for all n , then $I_n > 1 - O(\epsilon)$ for all n , in the sense that there exists a function f which is $O(\epsilon)$ and $T_n < \epsilon \Rightarrow I_n > 1 - f(\epsilon)$ for all n .
- 6) If $T_n > 1 - \epsilon$ for all n , then $I_n < O(\epsilon)$ for all n , in the sense that there exists a function g which is $O(\epsilon)$ and $T_n > 1 - \epsilon \Rightarrow I_n < g(\epsilon)$ for all n .

Then $I_\infty = \lim_{n \rightarrow \infty} I_n$ and $T_\infty = \lim_{n \rightarrow \infty} T_n$ both exist with probability 1 and take values in $\{0, 1\}$.

Proof: The proof follows from Lemma 2 of [2]. A sufficient condition for I_n to converge is when I_n is a bounded super-martingale. Note that condition (i&t.1) of Lemma 2 of [2] can be recovered from the last two conditions of this lemma. We use this notation to be consistent throughout the paper. To see this, note that (5) and (6) imply that there exist functions $f(\cdot), g(\cdot) : \mathbb{R} \rightarrow \mathbb{R}$ such that $\lim_{\delta \downarrow 0} f(\delta) = 0$

and $\lim_{\delta \downarrow 0} g(\delta) = 0$ and that $T_n < \delta$ implies $I_n > 1 - f(\delta)$ and $T_n > 1 - \delta$ implies $I_n < g(\delta)$. For an arbitrary $\epsilon > 0$, since the limit of both functions at zero is zero, let $\delta > 0$ be such that $f(\delta) < \epsilon$ and $g(\delta) < \epsilon$. For this choice of δ we have

$$T_n < \delta \Rightarrow I_n > 1 - f(\delta) > 1 - \epsilon$$

$$T_n > 1 - \delta \Rightarrow I_n < g(\delta) < \epsilon$$

Hence for any (sufficiently small) $\epsilon > 0$, there exists a $\delta > 0$ such that $T_n < \delta$ implies $I_n > 1 - \epsilon$ and $T_n > 1 - \delta$ implies $I_n < \epsilon$. Equivalently, for any $\epsilon > 0$, there exists a $\delta > 0$ such that $\epsilon \leq I_n \leq 1 - \epsilon$ implies $\delta \leq T_n \leq 1 - \delta$. \blacksquare

In the next lemma, we show that for any $d \in \mathbf{G}$, the random process Z_d^n converges to a Bernoulli random variable.

Lemma IV.3. *For all $d \in \mathbf{G}$, $Z_d^n(W)$ converges to a $\{0, 1\}$ -valued random variable $Z_d^\infty(W)$ as n grows. Moreover, if $\tilde{d} \in \mathbf{G}$ is such that $\langle \tilde{d} \rangle = \langle d \rangle$ then $Z_{\tilde{d}}^\infty(W) = Z_d^\infty(W)$ almost surely; i.e. the random processes $Z_{\tilde{d}}^n(W)$ and $Z_d^n(W)$ converge to the same random variable.*

Proof: This lemma has been proved in [2, Theorem 1] for $d = \arg \max_{a \neq 0} Z_a(W)$ when the underlying group is a field. The proof for an arbitrary d and an arbitrary group is given in the following. Let $H = \langle d \rangle$ be the subgroup of \mathbf{G} generated by d and let M be a maximal subgroup of H . Then the proof provided in [2] suffices for this lemma if we consider the quotient group H/M which is of prime order. We will elaborate on this in the following: Let

$$d' = \arg \max_{\substack{a \in H \\ a \notin M}} Z_a(W) \tag{10}$$

In Lemma IV.2, let I^n (Here we use the notation I^n instead of I_n for notational convenience) be equal to the process $I_H^n(W) - I_M^n(W)$ where $I_H^n(W)$ and $I_M^n(W)$ are defined by Equation (9) and let T_n be equal to the process $Z_{d'}^n(W)$ defined in (8). We claim that I^n and T_n satisfy the conditions of Lemma IV.2. The proof is given in the following:

Note that in the case of \mathbb{Z}_p fields, the only maximal subgroup of the group is the trivial subgroup $\{0\}$. Hence, (10) can be viewed as a straightforward generalization of the the definition made in [2]. Let M be a maximal subgroup of $H = \langle d \rangle$. Recall that a uniform random variable X over \mathbf{G} can be decomposed into two uniform and independent random variables \tilde{X} taking values from H and \hat{X} taking values from the transversal of H in \mathbf{G} . Similarly, the uniform random variable \tilde{X} over H can be

decomposed into two uniform and independent random variables \tilde{X} taking values from $M \leq H$ and \hat{X} taking values from the transversal of M in H . Using the chain rule we have:

$$\begin{aligned} I(\tilde{X}; Y|\hat{X}) &= I(\tilde{X}\hat{X}; Y|\hat{X}) \\ &= I(\hat{X}; Y|\hat{X}) + I(\tilde{X}; Y|\hat{X}\hat{X}) \end{aligned}$$

Note that $\tilde{X} \in M$ and (\hat{X}, \hat{X}) indicate the coset of M in \mathbf{G} to which X belongs. Therefore, the equation above implies that for each n , $I_H^n(W) - I_M^n(W) = I(\hat{X}; Y|\hat{X})$ where X and Y are the input and the output of the channel $W_N^{(J_n)}$. Since \hat{X} can at most take $\frac{|H|}{|M|}$ values, by choosing the base of the log function to be equal to $\frac{|H|}{|M|}$ condition (1) of Lemma IV.2 satisfies.

We have shown in Lemma IV.1 that both processes $I_H^n(W)$ and $I_M^n(W)$ are super-martingales and hence both converge almost surely. This means that the vector valued random process $(I_H^n(W), I_M^n(W))$ converges almost surely (refer to Proposition 5.25 of [8]). Hence condition (2) is satisfied.

Condition (3) trivially holds and condition (4) is shown to be satisfied in the proof of Theorem 1 of [2].

To show (5), assume $Z_{d'}^n(W) < \epsilon$. Let T_H be a transversal of H in \mathbf{G} and let T_M be a transversal of M in H . Given $X \in t_H + H$ for some $t_H \in T_H$, the joint probability distribution of cosets of M in $t_H + H$ and the channel output is given by:

$$\begin{aligned} \bar{p}(t_H + t_M + M, y) &\triangleq \sum_{m \in M} P(X = t_H + t_M + m, Y = y | X \in t_H + H) \\ &= \sum_{m \in M} \frac{P(X = t_H + t_M + m, Y = y)}{P(X \in t_H + H)} \\ &= \sum_{m \in M} \frac{P(X = t_H + t_M + m, Y = y)}{|H|/|\mathbf{G}|} \\ &= \frac{|\mathbf{G}|}{|H|} \sum_{m \in M} \frac{1}{|\mathbf{G}|} W(y | t_H + t_M + m) \\ &= \frac{1}{|H|} \sum_{m \in M} W(y | t_H + t_M + m) \end{aligned}$$

where t_M takes values from T_M . The corresponding channel is defined as:

$$\begin{aligned}\bar{W}(y|t_H + t_M + M) &= \frac{1}{P(X \in t_H + t_M + M | X \in t_H + H)} \frac{1}{|H|} \sum_{m \in M} W(y|t_H + t_M + m) \\ &= \frac{1}{|M|} \sum_{m \in M} W(y|t_H + t_M + m)\end{aligned}\quad (11)$$

Note that the input of this channel takes values from the set $\{t_H + t_M + M | t_M \in T_M\}$ uniformly and the size of the input alphabet is $\frac{|H|}{|M|} \triangleq \bar{q}$ which is a prime (since M is maximal in H). Furthermore, by definition $I(\bar{W}) = I(\hat{X}; Y | \hat{X} = t_H)$. It is shown in Appendix C that $Z_{d'}(W) < \epsilon$ implies $Z(\bar{W}) < C\epsilon$ for some constant $C = \frac{|M| \cdot |H| \cdot |G|}{|H| - |M|}$. Therefore, [2, Prop. 3] implies $I(\bar{W}) = \log \frac{|H|}{|M|} - O(\epsilon)$. This result is valid for all $t_H \in T_H$. Therefore

$$\begin{aligned}I_H(W) - I_M(W) &= \sum_{t_H \in T_H} P(\hat{X} = t_H) I(\hat{X}; Y | \hat{X} = t_H) \\ &= \log \frac{|H|}{|M|} - O(\epsilon)\end{aligned}$$

To show condition (6), assume that $Z_{d'}^n(W) > 1 - \epsilon$. For the channel \bar{W} defined as above, it is shown in Appendix D (An alternate proof for the \mathbb{Z}_{p^r} case can be found in Appendix E) that $Z_{d'}(W) > 1 - \epsilon$ implies $Z_{d'+t_H+M}(\bar{W}) > 1 - \frac{2q(2\epsilon-\epsilon^2)}{\bar{q}|M|} = 1 - O(\epsilon)$. Since the input alphabet of the channel \bar{W} has a prime size and $d' \in H \setminus M$, we can use [2, Lemma 4] to conclude that $Z(\bar{W}) > 1 - \frac{2q\bar{q}^2(2\epsilon-\epsilon^2)}{|M|} = 1 - O(\epsilon)$. Now we use [2, Prop. 3] to conclude $I(\bar{W}) < O(\epsilon)$. This implies:

$$\begin{aligned}I_H(W) - I_M(W) &= \sum_{t_H \in T_H} P(\hat{X} = t_H) I(\hat{X}; Y | \hat{X} = t_H) \\ &< O(\epsilon)\end{aligned}$$

So far, we have shown that for any $d \in G$, for $H = \langle d \rangle$ and d' defined as in (10), the random variable $Z_{d'}^n(W)$ converges to a Bernoulli random variable. Note that so far the proof is general and applies to arbitrary groups as well. We will use this part of the proof later in Section V. Next, we show that when $G = \mathbb{Z}_{p^r}$, for any $\tilde{d} \in H \setminus M$ (including d itself), $Z_{\tilde{d}}^n(W)$ converges to a Bernoulli random variable. Moreover, all such \tilde{d} 's converge to the same random variable. To see this, note that if $Z_{d'}^n < \epsilon$, it follows that $Z_{\tilde{d}}^n < \epsilon$ for all $\tilde{d} \in H \setminus M$ and if $Z_{d'}^n > 1 - \epsilon$ we show that for all $\tilde{d} \in \langle d' \rangle = H$, $Z_{\tilde{d}}^n > 1 - O(\epsilon)$. For any $\tilde{d} \in H = \langle d \rangle$ we can write $\tilde{d} = id'$ for some integer i . The condition $Z_{d'} > 1 - \epsilon$ implies $1 - Z(W_{\{x, x+d'\}}) \leq q\epsilon$ for all $x \in \mathbf{G}$. It has been shown in the proof of [2, Lemma 4] that

$$\sqrt{1 - Z(W_{\{x, x+2d'\}})} \leq \sqrt{1 - Z(W_{\{x, x+d'\}})} + \sqrt{1 - Z(W_{\{x+d, x+2d'\}})} \leq 2\sqrt{q\epsilon}$$

Repeated application of this inequality for i times yields $\sqrt{1 - Z(W_{\{x, x+\tilde{d}\}})} \leq i\sqrt{q\epsilon} \leq q\sqrt{q\epsilon}$ or equivalently $Z(W_{\{x, x+\tilde{d}\}}) \geq 1 - q^3\epsilon$. It then follows that $Z_{\tilde{d}} \geq 1 - q^3\epsilon$. Note that when $\mathbf{G} = \mathbb{Z}_{p^r}$, $H \setminus M$ is the set of all elements \tilde{d} such that $\langle \tilde{d} \rangle = \langle d \rangle$. This completes the proof of the lemma. ■

The next lemma gives a sufficient condition for two processes Z_d^n and $Z_{\tilde{d}}^n$ to converge to the same random variable. Recall that for $0 \leq t \leq r-1$, $K_t = H_t \setminus H_{t+1}$.

Lemma IV.4. *If $d, \tilde{d} \in K_t$ for some $0 \leq t \leq r-1$, then Z_d^n and $Z_{\tilde{d}}^n$ converge to the same Bernoulli random variable.*

Proof: Note that $d, \tilde{d} \in K_t$ implies $\langle d \rangle = \langle \tilde{d} \rangle = H_t$. Therefore, Lemma IV.3 implies Z_d^n and $Z_{\tilde{d}}^n$ converge to the same Bernoulli random variable. ■

For $t = 0, 1, \dots, r-1$, pick an arbitrary element $k_t \in K_t$. The lemma above suggests that we only need to study Z_{k_t} 's rather than all Z_d 's.

Lemma IV.5. *If $Z_{k_t} > 1 - \epsilon$ then $Z_{k_s} \approx_\epsilon 1$ for all $t \leq s \leq r-1$.*

Proof: Note that $k_s \in \langle k_t \rangle$ and let $d = k_t$ and $k_s = id$ for some integer i . The condition $Z_{k_t} > 1 - \epsilon$ implies $1 - Z(W_{\{x, x+d\}}) \leq q\epsilon$ for all $x \in \mathbf{G}$. It has been shown in the proof of [2, Lemma 4] that for all $x \in \mathbf{G}$

$$\sqrt{1 - Z(W_{\{x, x+2d\}})} \leq 2\sqrt{q\epsilon}$$

Repeated application of this inequality for i times yields $\sqrt{1 - Z(W_{\{x, x+k_s\}})} \leq i\sqrt{q\epsilon}$ for all $x \in \mathbf{G}$. It follows that $Z_{k_s} \geq 1 - O(\epsilon)$. ■

This lemma implies that for the group $\mathbf{G} = \mathbb{Z}_{p^r}$ all possible asymptotic cases are:

- **Case 0:** $Z_{k_0} = 1, Z_{k_1} = 1, Z_{k_2} = 1, \dots, Z_{k_{r-1}} = 1$
- **Case 1:** $Z_{k_0} = 0, Z_{k_1} = 1, Z_{k_2} = 1, \dots, Z_{k_{r-1}} = 1$
- **Case 2:** $Z_{k_0} = 0, Z_{k_1} = 0, Z_{k_2} = 1, \dots, Z_{k_{r-1}} = 1$
- \vdots
- **Case r:** $Z_{k_0} = 0, Z_{k_1} = 0, Z_{k_2} = 0, \dots, Z_{k_{r-1}} = 0,$

where for $t = 0, \dots, r$, case t happens with some probability p_t .

Next, we study the behavior of I^n in each of these asymptotic cases.

Lemma IV.6. *For a channel $(\mathbb{Z}_{p^r}, \mathcal{Y}, W)$ and for $t = 0, 1, \dots, r$, if $Z_{k_0} < \epsilon, Z_{k_1} < \epsilon, \dots, Z_{k_{t-1}} < \epsilon, Z_{k_t} > 1 - \epsilon, \dots, Z_{k_{r-1}} > 1 - \epsilon$, then $t \log p - O(\epsilon) < I^0(W) < t \log p + O(\epsilon)$.*

Proof: Note that for all $s = 0, \dots, r-1$, $M_s \triangleq \langle k_{s+1} \rangle$ is a maximal subgroup of $\langle k_s \rangle$. In the proof of Lemma IV.3, if we let $d = k_0$ and $M_0 = \langle k_1 \rangle$, we get $I_{\mathbf{G}}(W) - I_{M_0}(W) = I(W) - I_{M_0}(W) \approx_{\epsilon} \log p$ (Here we take the base of the log function to be equal to 2). Similarly, it follows that $I_{M_s}(W) - I_{M_{s+1}}(W) \approx_{\epsilon} \log p$ for all $0 \leq s \leq t-1$. For $s \geq t$ we have, $I_{M_s} - I_{M_{s+1}} \approx_{\epsilon} 0$. Therefore,

$$\begin{aligned} I^0(W) &= I_{\mathbf{G}}(W) = \sum_{s=0}^{r-1} I_{M_s}(W) - I_{M_{s+1}}(W) \\ &= \sum_{s=0}^{t-1} I_{M_s}(W) - I_{M_{s+1}}(W) + \sum_{s=t}^{r-1} I_{M_s}(W) - I_{M_{s+1}}(W) \\ &\approx_{\epsilon} \sum_{s=0}^{t-1} \log p + \sum_{s=t}^{r-1} 0 \\ &= t \log p \end{aligned}$$

■

We have shown that the process I^n converges to the following $r+1$ valued discrete random variable: $I^{\infty} = t \log p$ with probability p_t for $t = 0, \dots, r$.

For $t = 0, \dots, r$, define the random variable $Z^t(W_N^{(i)}) = \sum_{d \notin H_t} Z_d(W_N^{(i)})$ and the random process $(Z^t)^{(n)}(W) = Z^t(W_N^{(J_n)})$ where J_n is a uniform random variable over $\{1, 2, \dots, N = 2^n\}$. Note that $(Z^t)^{(n)}(W)$ converges to a random variable $(Z^t)^{(\infty)}(W)$ almost surely and $P((Z^t)^{(\infty)} = 0) = \sum_{s=t}^r p_s$.

3) *Summary of Channel Transformation:* For the channel $(\mathbb{Z}_{p^r}, \mathcal{Y}, W)$, consider the vector random process $\mathbf{V}^n = (Z_{k_0}^n, Z_{k_1}^n, \dots, Z_{k_{r-1}}^n, I^n)$. We have seen in the previous section that each component of this vector random process converges almost surely. Proposition 5.25 of [8] implies that the vector random process \mathbf{V}^n also converges almost surely to a random vector \mathbf{V}^{∞} . The random vector \mathbf{V}^{∞} is a discrete random variable defined as follows:

$$P \left(\mathbf{V}^{\infty} = (\underbrace{0, \dots, 0}_{t \text{ times}}, \underbrace{1, \dots, 1}_{r-t \text{ times}}, t \log p) \right) = p_t$$

for $t = 0, 1, \dots, r$ where p_t 's are some probabilities. This implies that for all $\epsilon > 0$, there exists a number $N = N(\epsilon) = 2^{n(\epsilon)}$ and a partition $\{A_0^{\epsilon}, A_1^{\epsilon}, \dots, A_r^{\epsilon}\}$ of $\{1, \dots, N\}$ such that for $t = 0, \dots, r$ and $i \in A_t^{\epsilon}$, $Z_{k_s}(W_N^{(i)}) < O(\epsilon)$ if $0 \leq s < t$ and $Z_{k_s}(W_N^{(i)}) > 1 - O(\epsilon)$ if $t \leq s < r$. For $t = 0, \dots, r$ and $i \in A_t^{\epsilon}$, we have $I(W_N^{(i)}) = t \log(p) + O(\epsilon)$ and $Z^t(W_N^{(i)}) = O(\epsilon)$. Moreover, as $\epsilon \rightarrow 0$, $\frac{|A_t^{\epsilon}|}{N} \rightarrow p_t$ for some probabilities p_0, \dots, p_r .

In Appendix F, we show that for any $\beta < \frac{1}{2}$ and for $t = 0, \dots, r$,

$$\begin{aligned} \lim_{n \rightarrow \infty} P\left((Z^t)^{(n)} < 2^{-2^{\beta n}}\right) &\geq P\left((Z^t)^{(\infty)} = 0\right) \\ &= \sum_{s=t}^r p_s \end{aligned} \quad (12)$$

Remark IV.1. *This observation implies the following stronger result: For all $\epsilon > 0$, there exists a number $N = N(\epsilon) = 2^{n(\epsilon)}$ and a partition $\{A_0^\epsilon, A_1^\epsilon, \dots, A_r^\epsilon\}$ of $\{1, \dots, N\}$ such that for $t = 0, \dots, r$ and $i \in A_t^\epsilon$, $I(W_N^{(i)}) = t \log(p) + O(\epsilon)$ and $Z^t(W_N^{(i)}) < 2^{-2^{\beta n(\epsilon)}}$. Moreover, as $\epsilon \rightarrow 0$, $\frac{|A_t^\epsilon|}{N} \rightarrow p_t$ for some probabilities p_0, \dots, p_r .*

C. Encoding and Decoding

In the original construction of polar codes, we fix the input symbols corresponding to useless channels and send information symbols over perfect channels. Here, since the channels do not polarize into two levels, the encoding is slightly different and we send “some” information bits over “partially perfect” channels. At the encoder, if $i \in A_t^\epsilon$ for some $t = 0, \dots, r$, the information symbol is chosen from the transversal T_t arbitrarily and not from the whole set \mathbf{G} . As we will see later, the channel $W_N^{(i)}$ is perfect for symbols chosen from T_t and perfect decoding is possible at the decoder. Let $\mathcal{X}_N^\epsilon = \bigoplus_{t=0}^r T_t^{A_t^\epsilon}$ be the set of all valid input sequences. For the sake of analysis, as in the binary case, the message u_1^N is dithered with a uniformly distributed random vector $b_1^N \in \bigoplus_{t=0}^r H_t^{A_t^\epsilon}$ revealed to both the encoder and the decoder. A message $v_1^N \in \mathcal{X}_N^\epsilon$ is encoded to the vector $x_1^N = (v_1^N + b_1^N)G_N$. Note that $u_1^N = v_1^N + b_1^N$ is uniformly distributed over \mathbf{G}^N .

At the decoder, after observing the output vector y_1^N , for $t = 0, \dots, r$ and $i \in A_t^\epsilon$, use the following decoding rule:

$$\hat{u}_i = f_i(y_1^N, \hat{u}_1^{i-1}) = \arg \max_{g \in b_i + T_t} W_N^{(i)}(y_1^N, \hat{u}_1^{i-1} | g)$$

And finally, the message is decoded as $\hat{v}_1^N = \hat{u}_1^N - b_1^N$.

The total number of valid input sequences is equal to

$$2^{NR} = \prod_{t=0}^r |T_t|^{|A_t^\epsilon|} = \prod_{t=0}^r p^{t|A_t^\epsilon|} \approx \prod_{t=0}^r p^{tp_t N}$$

Therefore, the rate is equal to $R = \sum_{t=0}^r p_t t \log p$. On the other hand, since I^n is a martingale, we have $\mathbb{E}\{I^\infty\} = I^0$. Since $\mathbb{E}\{I^\infty\} = \sum_{t=0}^r p_t t \log p$, we observe that the rate R is equal to the symmetric capacity I^0 . We will see in the next section that this rate is achievable.

D. Error Analysis

Let B_i be the event that the first error occurs when the decoder decodes the i th symbol:

$$\begin{aligned} B_i &= \left\{ (u_1^N, y_1^N) \in \mathbf{G}^N \times \mathcal{Y}^N \mid \forall j < i : u_j = f_j(y_1^N, u_1^{j-1}), u_i \neq f_i(y_1^N, u_1^{i-1}) \right\} \\ &\subseteq \left\{ (u_1^N, y_1^N) \in \mathbf{G}^N \times \mathcal{Y}^N \mid u_i \neq f_i(y_1^N, u_1^{i-1}) \right\} \end{aligned} \quad (13)$$

For $t = 0, \dots, r$ and $i \in A_t^\epsilon$, define

$$\begin{aligned} E_i &= \left\{ (u_1^N, y_1^N) \in \mathbf{G}^N \times \mathcal{Y}^N \mid W_N^{(i)}(y_1^N, u_1^{i-1} \mid u_i) \right. \\ &\quad \left. \leq W_N^{(i)}(y_1^N, u_1^{i-1} \mid \tilde{u}_i) \text{ for some } \tilde{u}_i \in b_i + T_t, \tilde{u}_i \neq u_i \right\} \end{aligned} \quad (14)$$

Lemma IV.7. For $t = 0, \dots, r$ and $i \in A_t^\epsilon$, $P(E_i) \leq q^2 Z^t(W_N^{(i)})$.

Proof: For $u_i \in \mathbf{G}$, write $u_i = b_i(u_i) + v_i(u_i)$ where $b_i(u_i) \in H_t$ and $v_i(u_i) \in T_t$. We have

$$\begin{aligned} P(E_i) &= \sum_{u_1^N, y_1^N} \frac{1}{q^N} W_N(y_1^N \mid u_1^N) \mathbf{1}_{E_i}(u_1^N, y_1^N) \\ &\leq \sum_{u_1^N, y_1^N} \frac{1}{q^N} W_N(y_1^N \mid u_1^N) \sum_{\tilde{u}_i \in b_i(u_i) + T_t, \tilde{u}_i \neq u_i} \sqrt{\frac{W_N^{(i)}(y_1^N, u_1^{i-1} \mid \tilde{u}_i)}{W_N^{(i)}(y_1^N, u_1^{i-1} \mid u_i)}} \\ &= \sum_{u_1^i, y_1^i} \frac{1}{q} \left(\sum_{u_{i+1}^N} \frac{1}{q^{N-1}} W_N(y_1^N \mid u_1^N) \right) \sum_{\tilde{u}_i \in b_i(u_i) + T_t, \tilde{u}_i \neq u_i} \sqrt{\frac{W_N^{(i)}(y_1^N, u_1^{i-1} \mid \tilde{u}_i)}{W_N^{(i)}(y_1^N, u_1^{i-1} \mid u_i)}} \\ &= \sum_{u_1^i, y_1^i} \frac{1}{q} W_N^{(i)}(y_1^N, u_1^{i-1} \mid u_i) \sum_{\tilde{u}_i \in b_i(u_i) + T_t, \tilde{u}_i \neq u_i} \sqrt{\frac{W_N^{(i)}(y_1^N, u_1^{i-1} \mid \tilde{u}_i)}{W_N^{(i)}(y_1^N, u_1^{i-1} \mid u_i)}} \\ &= \sum_{u_i \in \mathbf{G}} \sum_{\tilde{u}_i \in b_i(u_i) + T_t, \tilde{u}_i \neq u_i} \frac{1}{q} \sum_{u_1^{i-1}, y_1^{i-1}} \sqrt{W_N^{(i)}(y_1^{i-1}, u_1^{i-2} \mid \tilde{u}_i) W_N^{(i)}(y_1^{i-1}, u_1^{i-2} \mid u_i)} \\ &= \sum_{u_i \in \mathbf{G}} \sum_{\tilde{u}_i \in b_i(u_i) + T_t, \tilde{u}_i \neq u_i} \frac{1}{q} Z_{\{u_i, \tilde{u}_i\}}(W_N^{(i)}) \end{aligned}$$

For $u_i \in \mathbf{G}$ and $\tilde{u}_i \in b_i(u_i) + T_t$, if $u_i \neq \tilde{u}_i$, then u_i, \tilde{u}_i are not in the same coset of H_t and hence $u_i - \tilde{u}_i \notin H_t$. Therefore, $u_i - \tilde{u}_i \in \mathbf{G} \setminus H_t$. Note that for $d = u_i - \tilde{u}_i$, $Z_{\{u_i, \tilde{u}_i\}}(W_N^{(i)}) \leq q Z_d(W_N^{(i)})$. Since $d \in \mathbf{G} \setminus H_t$, we have $Z_d(W_N^{(i)}) \leq Z^t(W_N^{(i)})$ and hence,

$$Z_{\{u_i, \tilde{u}_i\}}(W_N^{(i)}) \leq q Z^t(W_N^{(i)})$$

Therefore, $P(E_i) \leq q |T_t| Z^t(W_N^{(i)}) \leq q^2 Z^t(W_N^{(i)})$. ■

The probability of block error is given by $P(err) = \sum_{t=0}^r \sum_{i \in A_t^\epsilon} P(B_i)$. Since $B_i \subseteq E_i$, we get

$$P(err) \leq \sum_{t=0}^r \sum_{i \in A_t^\epsilon} q^2 Z^t(W_N^{(i)}) \quad (15)$$

$$\stackrel{(a)}{\leq} \sum_{t=0}^r |A_t^\epsilon| q^2 2^{-2\beta n} \quad (16)$$

$$\leq q^2 N 2^{-2\beta n} \quad (17)$$

for any $\beta < \frac{1}{2}$ where (a) follows from Remark IV.1. Therefore, the probability of error goes to zero as $\epsilon \rightarrow 0$ (and hence $n \rightarrow \infty$).

V. POLAR CODES OVER ARBITRARY CHANNELS

For any channel input alphabet there always exist an Abelian group of the same size. In this section, we generalize the result of the previous section to channels of arbitrary input alphabet sizes and arbitrary group operations.

A. Abelian Groups

Let the Abelian group \mathbf{G} be the input alphabet of the channel. It is a standard fact that any Abelian group can be decomposed into a direct sum of \mathbb{Z}_{p^r} rings [9]. Let $\mathbf{G} = \bigoplus_{l=1}^L \mathbf{R}_l$ with $\mathbf{R}_l = \mathbb{Z}_{p_l^{r_l}}$ where p_l 's are prime numbers and r_l 's are positive integers. For $t = (t_1, t_2, \dots, t_L)$ with $t_l \in \{0, 1, \dots, r_l\}$, there exists a corresponding subgroup H of \mathbf{G} defined by $H = \bigoplus_{l=1}^L p_l^{t_l} \mathbf{R}_l$. For a subgroup H of \mathbf{G} define T_H to be a transversal of H in \mathbf{G} .

B. Recursive Channel Transformation

1) *The Basic Channel Transforms:* The transformed channels W^+ and W^- and the process $I^n(W)$ are defined the same way as the \mathbb{Z}_{p^r} case through Equations (5), (6) and (7).

2) *Asymptotic Behavior of Synthesized Channels:* For $d \in \mathbf{G}$, define $Z_d^n(W)$ same as (8) where $q = |\mathbf{G}|$ and for $H \leq \mathbf{G}$, define $I_H^n(W)$ by Equation (9). To prove the polarization for arbitrary groups, we need the following lemma:

Lemma V.1. *For $d_1, d_2 \in \mathbf{G}$, if $Z_{d_1}(W) > 1 - \epsilon$ and $Z_{d_2}(W) > 1 - \epsilon$, then $Z_{\tilde{d}}(W) \approx_\epsilon 1$ for any $\tilde{d} \in \langle d_1, d_2 \rangle$ where $\langle d_1, d_2 \rangle$ is the subgroup of \mathbf{G} generated by d_1 and d_2 .*

Proof: The condition $Z_{d_1} > 1 - \epsilon$ implies $1 - Z(W_{\{x, x+d_1\}}) \leq q\epsilon$ and the condition $Z_{d_2} > 1 - \epsilon$ implies $1 - Z(W_{\{x, x+d_2\}}) \leq q\epsilon$. Similar to the proof of Lemma IV.5, we have

$$\sqrt{1 - Z(W_{\{x, x+2d_1\}})} \leq 2\sqrt{q\epsilon}, \quad \sqrt{1 - Z(W_{\{x, x+2d_2\}})} \leq 2\sqrt{q\epsilon}$$

It is also straightforward to show that

$$\sqrt{1 - Z(W_{\{x, x+d_1+d_2\}})} \leq 2\sqrt{q\epsilon}$$

Since $\tilde{d} \in \langle d_1, d_2 \rangle$, it can be written as $\tilde{d} = id_1 + jd_2$ for some integers i, j . Repeated application of the above inequalities yields the lemma. \blacksquare

Remark V.1. *This lemma is generalizable to the case where for $d_1, \dots, d_m \in \mathbf{G}$, $Z_{d_1}(W) > 1 - \epsilon$, $Z_{d_2}(W) > 1 - \epsilon, \dots, Z_{d_m}(W) > 1 - \epsilon$. In this case, we have $Z_{\tilde{d}}(W) \approx_\epsilon 1$ for any $\tilde{d} \in \langle d_1, d_2, \dots, d_m \rangle$.*

The following lemma is a restatement of Lemma IV.3. Here, we prove it for arbitrary groups.

Lemma V.2. *For all $d \in \mathbf{G}$, $Z_d^n(W)$ converges to a $\{0, 1\}$ -valued random variable $Z_d^\infty(W)$ as n grows. Moreover, if $\tilde{d} \in \mathbf{G}$ is such that $\langle \tilde{d} \rangle = \langle d \rangle$ then $Z_{\tilde{d}}^\infty(W) = Z_d^\infty(W)$ almost surely; i.e. the random processes $Z_{\tilde{d}}^n(W)$ and $Z_d^n(W)$ converge to the same random variable.*

Proof: Similar to the proof of Lemma IV.3, let $H = \langle d \rangle$ and let M be any maximal subgroup of H . Define

$$d' = \arg \max_{\substack{a \in H \\ a \notin M}} Z_a(W) \quad (18)$$

It is relatively straightforward to show that in the general case as well, $Z_{d'}^n(W)$ converges to a $\{0, 1\}$ -valued random variable $Z_{d'}^\infty(W)$. Indeed this part of the proof of Lemma IV.3 is general enough for arbitrary Abelian groups. Here we show that this implies $Z_d^n(W)$ also converges to a Bernoulli random variable.

Let $|H| = \prod_{i=1}^k q_i^{a_i}$ where q_i 's are distinct primes and a_i 's are positive integers. Note that H is isomorphic to the cyclic group $\mathbb{Z}_{|H|}$. For $i = 1, \dots, k$, define the subgroup $M_i = \langle q_i \rangle$ of $\mathbb{Z}_{|H|}$ (and isomorphically of H) and let $d'_i = \arg \max_{\substack{a \in H \\ a \notin M_i}} Z_a(W)$. Note that for $i = 1, \dots, k$, M_i is a maximal subgroup of $\mathbb{Z}_{|H|}$ (and isomorphically of H). Therefore, for $i = 1, \dots, k$, $Z_{d'_i}^n(W)$ converges to a $\{0, 1\}$ -valued random variable. If for some $i = 1, \dots, k$, $Z_{d'_i}(W) < \epsilon$ it follows that $Z_d(W) < \epsilon$ (since $d \in H \setminus M_i$) and if for all $i = 1, \dots, k$, $Z_{d'_i}(W) > 1 - \epsilon$, it follows from Remark V.1 that $Z_{\tilde{d}}(W) > 1 - O(\epsilon)$ for

any $\tilde{d} \in \langle d'_1, d'_2, \dots, d'_k \rangle$. Next, we show that $\langle d'_1, d'_2, \dots, d'_k \rangle = H$ and this will prove that if for all $i = 1, \dots, k$, $Z_{d'_i}(W) > 1 - \epsilon$ then $Z_d(W) > 1 - O(\epsilon)$. For $i = 1, \dots, k$, since $d'_i \notin M_i$ it follows that $d'_i \not\equiv 0 \pmod{q_i}$. Define

$$\delta = \sum_{i=1}^k \left(\prod_{\substack{j=1 \\ j \neq i}}^k q_j \right) d'_i$$

Then we have $\delta \not\equiv 0 \pmod{q_i}$ for all $i = 1, \dots, k$. This implies $\langle \delta \rangle = H$ and hence $\langle d'_1, d'_2, \dots, d'_k \rangle = H$. Therefore, if in the limit $Z_{d'_i}(W) = 0$ for some $i = 1, \dots, k$ then $Z_d(W) = 0$ and if $Z_{d'_i}(W) = 0$ for all $i = 1, \dots, k$ then $Z_d(W) = 1$. This proves that $Z_d^n(W)$ converges to a Bernoulli random variable.

If $\tilde{d} \in \mathbf{G}$ is such that $\langle \tilde{d} \rangle = \langle d \rangle$ then it follows that $\tilde{d} \in H$ and $\tilde{d} \notin M_i$ for $i = 1, \dots, k$. Therefore if in the limit $Z_{d'_i}(W) = 0$ for some $i = 1, \dots, k$ then $Z_{\tilde{d}}(W) = 0$ and if $Z_{d'_i}(W) = 0$ for all $i = 1, \dots, k$ then $Z_{\tilde{d}}(W) = 1$. This proves that the random processes $Z_d^n(W)$ and $Z_{\tilde{d}}^n(W)$ converge to the same random variable. \blacksquare

In the asymptotic regime, let d_1, d_2, \dots, d_m be all elements of \mathbf{G} such that $Z_{d_i}(W) = 1$ and assume that for all other elements $d \in \mathbf{G}$, $Z_d(W) = 0$ (we can make this assumption since in the limit Z_d 's are $\{0, 1\}$ -valued). We have seen that if $Z_{d_i}(W) = 1$ for $i = 1, \dots, m$ then for any $\tilde{d} \in \langle d_1, d_2, \dots, d_m \rangle$, $Z_{\tilde{d}}(W) = 1$. Therefore, $\langle d_1, d_2, \dots, d_m \rangle \subseteq \{d_1, d_2, \dots, d_m\}$ and hence $\{d_1, d_2, \dots, d_m\} = \langle d_1, d_2, \dots, d_m \rangle = H$ for some subgroup H of \mathbf{G} . This means all possible asymptotic cases can be indexed by subgroups of \mathbf{G} . i.e. for any $H \leq \mathbf{G}$, one possible asymptotic case is

- **Case H :** $Z_d(W) = \begin{cases} 1 & \text{if } d \in H; \\ 0 & \text{Otherwise.} \end{cases}$

where for $H \leq \mathbf{G}$, case H happens with some probability p_H .

Next, We study the behavior of I^n in each of these cases.

Lemma V.3. *For a channel $(\mathbf{G}, \mathcal{Y}, W)$ and for a subgroup S of \mathbf{G} , if $Z_d > 1 - \epsilon$ for $d \in S$ and $Z_d < \epsilon$ for $d \notin S$, then $I^0(W) \approx_\epsilon \log \frac{|\mathbf{G}|}{|S|}$.*

Proof: Let $0 = M_0 \subseteq M_1 \subseteq \dots \subseteq M_{t-1} \subseteq S = M_t \subseteq M_{t+1} \subseteq \dots \subseteq \mathbf{G} = M_k$ for some positive integer k be any chain of subgroups such that M_{s-1} is maximal in M_s for $s = 1, \dots, k$.

For $s = 1, \dots, t$ let $H = M_s$ and $M = M_{s-1}$ and let T_H be a transversal of H in \mathbf{G} and let T_M be a transversal of M in H . For $d \in H$, we have $Z_d(W) > 1 - \epsilon$. For $t_H \in T_H$ define the channel

$\bar{W}(y|t_H + t_M + M_{s-1})$ similar to (11). We have shown in Appendix D that if for some $d \in H \setminus M$, $Z_d(W) > 1 - \epsilon$ then $Z_{d+t_H+M}(\bar{W}) > 1 - O(\epsilon)$. Since the input alphabet of the channel \bar{W} has a prime size, we can use [2, Lemma 4] to conclude that $Z(\bar{W}) > 1 - O(\epsilon)$. Now we use [2, Prop. 3] to conclude $I(\bar{W}) < O(\epsilon)$. This result is valid for all $t_H \in T_H$. Since $I(\bar{W}) = I(\hat{X}; Y | \hat{X} = t_H)$, we conclude that

$$\begin{aligned} I_H(W) - I_M(W) &= \sum_{t_H \in T_H} P(\hat{X} = t_H) I(\hat{X}; Y | \hat{X} = t_H) \\ &< O(\epsilon) \end{aligned}$$

Therefore, for $s = 1, \dots, t$, $I_{M_s}(W) - I_{M_{s-1}}(W) \approx_\epsilon 0$ and hence, $I_{M_t}(W) = I_S(W) \approx_\epsilon I_{M_0}(W) = 0$.

For $s = t + 1, \dots, k$ let $H = M_s$ and $M = M_{s-1}$ and let T_H be a transversal of H in \mathbf{G} and let T_M be a transversal of M in H . For $d \in H \setminus M$, we have $Z_d(W) < \epsilon$. For the channel \bar{W} defined as above, we have shown in Appendix C that if for all $d \in H \setminus M$, $Z_d(W) < \epsilon$ then $Z(\bar{W}) < O(\epsilon)$. Therefore, [2, Prop. 3] implies $I(\bar{W}) = \log \frac{|H|}{|M|} - O(\epsilon)$. Similar as above, we conclude that

$$I_H(W) - I_M(W) = \log \frac{|H|}{|M|} - O(\epsilon)$$

Therefore, for $s = t + 1, \dots, k$, $I_{M_s}(W) - I_{M_{s-1}}(W) \approx_\epsilon \log \frac{|M_s|}{|M_{s-1}|}$ and hence

$$\begin{aligned} I_{\mathbf{G}}(W) - I_S(W) &\approx_\epsilon \sum_{s=t+1}^k \log \frac{|M_s|}{|M_{s-1}|} \\ &= \log \frac{|\mathbf{G}|}{|S|} \end{aligned}$$

Since $I_S(W) \approx_\epsilon 0$, We conclude that $I^0(W) = I_{\mathbf{G}}(W) \approx_\epsilon \log \frac{|\mathbf{G}|}{|S|}$. ■

We have shown that the process I^n converges to the following discrete random variable: $I^\infty = \log \frac{|\mathbf{G}|}{|H|}$ with probability p_H for $H \leq \mathbf{G}$.

For $H \leq \mathbf{G}$, define the random variable $Z^H(W_N^{(i)}) = \sum_{d \notin H} Z_d(W_N^{(i)})$ and the random process $(Z^H)^{(n)}(W) = Z^H(W_N^{(J_n)})$ where J_n is a uniform random variable over $\{1, 2, \dots, N = 2^n\}$. Note that $(Z^H)^{(n)}(W)$ converges almost surely to a random variable $(Z^H)^{(\infty)}(W)$ and $P((Z^H)^{(\infty)} = 0) = \sum_{S \leq H} p_S$.

3) Summary of Channel Transformation: For the channel $(\mathbf{G}, \mathcal{Y}, W)$, the convergence of the processes I^n and $(Z^H)^n$ for $H \leq \mathbf{G}$ implies that for all $\epsilon > 0$, there exists a number $N = N(\epsilon)$ and a partition $\{A_H^\epsilon | H \leq \mathbf{G}\}$ of $\{1, \dots, N\}$ such that for $H \leq \mathbf{G}$ and $i \in A_H^\epsilon$, $I(W_N^{(i)}) = \log \frac{|\mathbf{G}|}{|H|} + O(\epsilon)$ and $Z^H(W_N^{(i)}) = O(\epsilon)$. Moreover, as $\epsilon \rightarrow 0$, $\frac{|A_H^\epsilon|}{N} \rightarrow p_H$ for some probabilities $p_H, H \leq \mathbf{G}$.

In Appendix F, we show that for any $\beta < \frac{1}{2}$ and for $H \leq \mathbf{G}$,

$$\begin{aligned} \lim_{n \rightarrow \infty} P\left((Z^H)^{(n)} < 2^{-2^{\beta n}}\right) &\geq P\left((Z^H)^{(\infty)} = 0\right) \\ &= \sum_{S \leq H}^r p_S \end{aligned} \quad (19)$$

This implies that for all $\epsilon > 0$, there exists a number $N = N(\epsilon) = 2^{n(\epsilon)}$ and a partition $\{A_H^\epsilon | H \leq \mathbf{G}\}$ of $\{1, \dots, N\}$ such that for $H \leq \mathbf{G}$ and $i \in A_H^\epsilon$, $I(W_N^{(i)}) = \log \frac{|\mathbf{G}|}{|H|} + O(\epsilon)$ and $Z^H(W_N^{(i)}) < 2^{-2^{\beta n(\epsilon)}}$. Moreover, as $\epsilon \rightarrow 0$, $\frac{|A_H^\epsilon|}{N} \rightarrow p_H$ for some probabilities $p_H, H \leq \mathbf{G}$.

C. Encoding and Decoding

At the encoder, if $i \in A_H^\epsilon$ for some $H \leq \mathbf{G}$, the information symbol is chosen from the transversal T_H arbitrarily. Let $\mathcal{X}_N^\epsilon = \bigoplus_{H \leq \mathbf{G}} T_H^{A_H^\epsilon}$ be the set of all valid input sequences. As in the \mathbb{Z}_{p^r} case, the message u_1^N is dithered with a uniformly distributed random vector $b_1^N \in \bigoplus_{H \leq \mathbf{G}} H^{A_H^\epsilon}$ revealed to both the encoder and the decoder. A message $v_1^N \in \mathcal{X}_N^\epsilon$ is encoded to the vector $x_1^N = (v_1^N + b_1^N)G_N$. Note that $u_1^N = v_1^N + b_1^N$ is uniformly distributed over \mathbf{G}^N .

At the decoder, after observing the output vector y_1^N , for $H \leq \mathbf{G}$ and $i \in A_H^\epsilon$, use the following decoding rule:

$$\hat{u}_i = f_i(y_1^N, \hat{u}_1^{i-1}) = \arg \max_{g \in b_i + T_H} W_N^{(i)}(y_1^N, \hat{u}_1^{i-1} | g)$$

And finally, the message is recovered as $\hat{v}_1^N = \hat{u}_1^N - b_1^N$.

The total number of valid input sequences is equal to

$$2^{NR} = \prod_{H \leq \mathbf{G}} |T_H|^{A_H} = \prod_{H \leq \mathbf{G}} \left(\frac{|\mathbf{G}|}{|H|} \right)^{|A_H|}$$

Therefore the rate is equal to $R = \sum_{H \leq \mathbf{G}} \frac{|A_H|}{N} \log \frac{|\mathbf{G}|}{|H|}$. On the other hand, since I^n is a martingale, we have $\mathbb{E}\{I^\infty\} = I^0$. Since $\mathbb{E}\{I^\infty\} = \sum_{H \leq \mathbf{G}} p_H \log \frac{|\mathbf{G}|}{|H|}$, we observe that the rate R converges to the symmetric capacity I^0 as $\epsilon \rightarrow 0$. We will see in the next section that this rate is achievable.

D. Error Analysis

For $H \leq G$ and $i \in A_H^\epsilon$, define the events B_i and E_i according to Equations (13) and (14). Similar to the \mathbb{Z}_{p^r} case, it is straightforward to show that for $H \leq G$ and $i \in A_H^\epsilon$, $P(E_i) \leq q^2 Z^H(W_N^{(i)})$ where $q = |\mathbf{G}|$. The probability of block error is given by $P(err) = \sum_{H \leq \mathbf{G}} \sum_{i \in A_H^\epsilon} P(B_i)$. Since $B_i \subseteq E_i$,

we get

$$\begin{aligned}
P(\text{err}) &\leq \sum_{H \leq \mathbf{G}} \sum_{i \in A_H^\epsilon} q^2 Z^H(W_N^{(i)}) \\
&\leq \sum_{H \leq \mathbf{G}} |A_H^\epsilon| q^2 2^{-2^{\beta n}} \\
&\leq q^2 N 2^{-2^{\beta n}}
\end{aligned}$$

for any $\beta < \frac{1}{2}$. Therefore, the probability of block error goes to zero as $\epsilon \rightarrow 0$ ($n \rightarrow \infty$).

VI. RELATION TO GROUP CODES

Recall that for an arbitrary group \mathbf{G} , the polar encoder of length N introduced in this paper maps the set $\bigoplus_{H \leq \mathbf{G}} T_H^{A_H}$ to \mathbf{G}^N where for a subgroup H of \mathbf{G} , T_H is a transversal of H and $\{A_H | H \leq \mathbf{G}\}$ is some partition of $\{1, \dots, N\}$. Note that the set of messages $\bigoplus_{H \leq \mathbf{G}} T_H^{A_H}$ is not necessarily closed under addition and hence in general, the set of encoder outputs is not a subgroup of \mathbf{G}^N ; i.e. polar codes constructed and analyzed in Sections IV and V are not group encoders. On the contrary, the standard polar codes (i.e. polar codes in which only perfect channels are used) are indeed group codes since their set of messages is of the form $\mathbf{G}^A \oplus \{0\}^{\{1, \dots, N\} \setminus A}$ for some $A \subseteq \{1, \dots, N\}$ which is closed under addition.

It is worth mentioning that polar encoders constructed in this paper fall into a larger class of structured codes called *nested group codes*. Nested group codes consist of two group codes: the inner code \mathbb{C}_i and the outer code \mathbb{C}_o such that the inner code is a subgroup of the outer code ($\mathbb{C}_i \leq \mathbb{C}_o$). The set of messages consists of cosets of \mathbb{C}_i in \mathbb{C}_o . For the case of polar codes, the inner code is given by

$$\begin{aligned}
\mathbb{C}_i &= \left[\bigoplus_{H \leq \mathbf{G}} H^{A_H} \right] G \\
&= \left\{ mG \mid m \in \bigoplus_{H \leq \mathbf{G}} H^{A_H} \right\}
\end{aligned}$$

and the outer code is the whole group space: $\mathbb{C}_o = \mathbf{G}^N$. To verify that this is indeed the case, it suffices to show that the set of codewords of polar codes $\left[\bigoplus_{H \leq \mathbf{G}} T_H^{A_H} \right] G$ has only one common element with each coset of \mathbb{C}_i . Equivalently, it suffices to show that for $m_1, m_2 \in \mathbf{G}^N$, if $m_1 G - m_2 G \in \mathbb{C}_i$, then either $m_1 \notin \bigoplus_{H \leq \mathbf{G}} T_H^{A_H}$ or $m_2 \notin \bigoplus_{H \leq \mathbf{G}} T_H^{A_H}$.

Lemma VI.1. *For $N = 2^n$ where n is a positive integer, the generator matrix corresponding to polar codes $G_N = B_N F^{\otimes n}$ is full rank.*

Proof: Since $G_N = B_N F^{\otimes n}$ where B_N is a permutation of rows, it suffices to show that $F^{\otimes n}$ is full rank. Note that the rank of the Kronecker product of two matrices is equal to the product of the ranks of matrices and the rank of F is equal to 2. Hence we have $\text{rank}(G) = \text{rank}(F^{\otimes n}) = 2^n = N$. ■

This lemma implies that if $m_1 G - m_2 G \in \mathbb{C}_i$ then $m_1 - m_2 \in \bigoplus_{H \leq \mathbf{G}} H^{A_H}$. This means either $m_1 \notin \bigoplus_{H \leq \mathbf{G}} T_H^{A_H}$ or $m_2 \notin \bigoplus_{H \leq \mathbf{G}} T_H^{A_H}$. This proves that polar codes are indeed nested group codes.

In this section, we consider two examples of channels over \mathbb{Z}_4 . The first example is Channel 1 introduced in Section III. Based on the symmetry of this channel, we show that polar codes achieve the group capacity of this specific channel. The intent of the second example is to show that in general, polar codes do not achieve the group capacity of channels. In order to find the capacity of polar codes as group codes, we use the standard construction of polar codes, i.e. we only use perfect channels and fix partially perfect and useless channels.

A. Example 1

Consider Channel 1 of Figure 1. Define $H_0 = \{0, 1, 2, 3\}$, $H_1 = \{0, 2\}$ and $H_2 = \{0\}$ and define $K_0 = \{1, 3\}$, $K_1 = \{2\}$ and $K_2 = \{0\}$. For this channel we have:

$$I^0 \triangleq I(X; Y) = 2 - \epsilon - 2\lambda$$

$$I_2^0 \triangleq I(X_1; Y) = 1 - (\epsilon + \lambda)$$

$$(I_2')^0 \triangleq I(X_1'; Y) = 1 - (\epsilon + \lambda) = I_2^0$$

where X is uniform over \mathbb{Z}_4 , X_1 is uniform over H_1 and X_1' is uniform over $1 + H_1$. The capacity of group codes over this symmetric channel is equal to [10]:

$$\begin{aligned} C &= \min(I_4^0, I_2^0 + (I_2')^0) = \min(2 - \epsilon - 2\lambda, 2 - 2\epsilon - 2\lambda) \\ &= 2 - 2\epsilon - 2\lambda \end{aligned}$$

All possible cases for this channel are

- **Case 0:** $Z_1^\infty = Z_3^\infty = 1, Z_2^\infty = 1$
- **Case 1:** $Z_1^\infty = Z_3^\infty = 0, Z_2^\infty = 1$
- **Case 2:** $Z_1^\infty = Z_3^\infty = 0, Z_2^\infty = 0$

As we saw in Figures 2 and 3, this result agrees with the asymptotic behavior of I^n predicted by the recursion formulas (1) and (2).

Define $I(W^{b_1 b_2 \dots b_n}) = I(X; Y)$ where X, Y are the input and output of $W^{b_1 b_2 \dots b_n}$ and X is uniform over \mathbb{Z}_4 . Similarly, define $I_2(W^{b_1 b_2 \dots b_n}) = I(X_1; Y)$ where X_1, Y are the input and output of $W^{b_1 b_2 \dots b_n}$ and X_1 is uniform over H_1 and define $I'_2(W^{b_1 b_2 \dots b_n}) = I(X'_1; Y)$ where X'_1, Y are the input and output of $W^{b_1 b_2 \dots b_n}$ and X'_1 is uniform over $1 + H_1$. Define the mutual information processes I_4^n, I_2^n and $(I'_2)^n$ to be equal to $I(W^{b_1 b_2 \dots b_n}), I_2(W^{b_1 b_2 \dots b_n})$ and $I'_2(W^{b_1 b_2 \dots b_n})$ where for $i = 1, \dots, n$, b_i 's are iid Bernoulli(0.5) random variables. For this channel, we can show that $I_2(W^{b_1 b_2 \dots b_n}) = I'_2(W^{b_1 b_2 \dots b_n}) = 1 - (\epsilon_n + \lambda_n)$ and conclude that $(I_2 + I'_2)^n \triangleq I_2^n + (I'_2)^n$ is a martingale. Therefore I_4^n and $(I_2 + I'_2)^n$ converge almost surely to random variables I_4^∞ and $(I_2 + I'_2)^\infty$ respectively. This observation provides us with an ad-hoc way to find the probabilities $p_t, t = 0, 1, 2$ of the limit random variable I_4^∞ for this simple channel. We can show the following for the final states:

- **case 0** $\Rightarrow I_4^\infty = 0, (I_2 + I'_2)^\infty = 0$
- **case 1** $\Rightarrow I_4^\infty = 1, (I_2 + I'_2)^\infty = 0$
- **case 2** $\Rightarrow I_4^\infty = 2, (I_2 + I'_2)^\infty = 2$

Therefore we obtain the following three equations:

$$\mathbb{E}\{I_4^\infty\} = p_0 \cdot 0 + p_1 \cdot 1 + p_2 \cdot 2 = I_4^0 = 2 - \epsilon - 2\lambda$$

$$\mathbb{E}\{(I_2 + I'_2)^\infty\} = p_0 \cdot 0 + p_1 \cdot 0 + p_2 \cdot 2 = (I_2 + I'_2)^0 = 2 - 2\epsilon - 2\lambda$$

$$p_0 + p_1 + p_2 = 1$$

Solving this system of equations, we obtain:

$$p_2 = 1 - \epsilon - \lambda = C/2$$

$$p_1 = I_4^0 - (I_2 + I'_2)^0$$

$$p_0 = 1 - (I_4^0 - (I_2 + I'_2)^0)/2$$

We see that the fraction of perfect channels is equal to the capacity of the channel achievable using group codes and therefore, polar codes achieve the capacity of group codes for this channel.

B. Example 2

The channel is depicted in Figure 7. We call This Channel 3. For this channel, when $\lambda = 0.2$ we have:

$$I^0 = I(X; Y) = 0.6390$$

$$(I_2^0 + I'_2)^0 = 0.2161$$

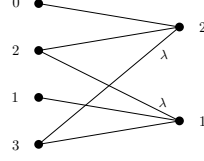


Fig. 7: Channel 3

The rate $C = \min(I_4^0, (I_2 + I_2')^0) = (I_2 + I_2')^0 = 0.2161$ is achievable using group codes over this channel [10].

For this channel we have three possible asymptotic case:

- **Case 0:** $Z_1^\infty = 1, Z_2^\infty = 1 \Rightarrow I_4^\infty = 0, (I_2 + I_2')^\infty = 0$
- **Case 1:** $Z_1^\infty = 0, Z_2^\infty = 1 \Rightarrow I_4^\infty = 1, (I_2 + I_2')^\infty = 0$
- **Case 2:** $Z_1^\infty = 0, Z_2^\infty = 0 \Rightarrow I_4^\infty = 2, (I_2 + I_2')^\infty = 2$

Therefore we obtain the following three equations:

$$\mathbb{E}\{I_4^\infty\} = p_0 \cdot 0 + p_1 \cdot 1 + p_2 \cdot 2$$

$$\mathbb{E}\{(I_2 + I_2')^\infty\} = p_0 \cdot 0 + p_1 \cdot 0 + p_2 \cdot 2$$

$$p_0 + p_1 + p_2 = 1$$

Therefore, the achievable rate using polar codes over this channel is equal to $R = 2p_2 = \mathbb{E}\{(I_2 + I_2')^\infty\}$.

We have $\mathbb{E}\{(I_2 + I_2')^1\} = 0.2063$ which is strictly less than $(I_2 + I_2')^0$. The following lemma implies $R = \mathbb{E}\{(I_2 + I_2')^\infty\} \leq \mathbb{E}\{(I_2 + I_2')^1\} < C = (I_2 + I_2')^0$ and completes the proof.

Lemma VI.2. *For a channel $(\mathbb{Z}_4, \mathcal{Y}, W)$, the process $(I_2 + I_2')^n, n = 0, 1, 2, \dots$ is a super-martingale.*

Proof: Follow from Lemma IV.1 with $H = \{0, 2\}$. ■

VII. CONCLUSION

It has been shown that the original construction of polar codes suffices to achieve the symmetric capacity of discrete memoryless channels with arbitrary input alphabet sizes. It is shown that in general, channel polarization happens in several levels so that some synthesized channels are partially perfect and there needs to be a modification of the coding scheme to exploit these channels. It has also been shown that polar codes do not generally achieve the capacity of arbitrary channels achievable using group codes.

APPENDIX

A. Polar Codes Over Abelian Groups

Given a $k \times n$ matrix G_n of 0's and 1's, one can construct a group code as follows: Given any message tuple $u^k \in G^k$, encode it to $u^k \cdot G_n$. Where the elements of G_n determine whether an element of u^k appears as a summand in the encoded word or not. For example consider the generator matrix

$$G_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Then $u^4 \cdot G_4$ is defined as

$$[u_1 u_2 u_3 u_4] \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} u_1 + u_2 + u_3 + u_4 \\ u_3 + u_4 \\ u_2 + u_4 \\ u_4 \end{pmatrix}$$

Using this convention, we can define a group code based on a given binary matrix without actually defining a multiplication operation for the group.

B. Recursion Formula for Channel 1

1) *Recursion for W^+* : We show that W^+ (corresponding to $b_1 = 1$) is equivalent to a channel of the same type as W but with different parameters ϵ_1 and λ_1 corresponding to ϵ and λ respectively; where,

$$\epsilon_1 = \epsilon^2 + 2\epsilon\lambda$$

$$\lambda_1 = \lambda_1^2$$

We say an output tuple (y_1, y_2, u_1) is connected to an input $u_2 \in \mathbb{Z}_4$ if $W^+(y_1, y_2, u_1 | u_2) = \frac{1}{4}W(y_1 | u_1 + u_2)W(y_2 | u_2)$ is strictly positive.

First, let us assume the output tuple (y_1, y_2, u_1) is connected to all $u_2 \in \mathbb{Z}_4$. Then $W(y_2 | u_2)$ must be nonzero for all u_2 and hence $y_2 = E_3$. Similarly since $W(y_1 | u_1 + u_2)$ is nonzero for all u_2 (and hence all $u_1 + u_2$) it follows that $y_1 = E_3$. Therefore $W^+(E_3, E_3, u_1 | u_2) = \frac{1}{4}\lambda^2$ for all $u_1, u_2 \in \mathbb{Z}_4$ and these are all output tuples connected to all inputs (with positive probability). Since all of these output tuples are equivalent we can combine them to get a single output symbol connected to all four inputs with

probability λ^2 .

Next we show that if an output tuple is connected to an input from $\{0, 2\}$ and an input from $\{1, 3\}$, then it is connected to all inputs. Consider the case where the output tuple (y_1, y_2, u_1) is connected to both 0 and 1 i.e. $W^+(y_1, y_2, u_1|0) \neq 0$ and $W^+(y_1, y_2, u_1|1) \neq 0$. Then since $W(y_2|0) \neq 0$ and $W(y_2|1) \neq 0$, it follows that $y_2 = E_3$. Similarly since $W(y_1|u_1) \neq 0$ and $W(y_1|u_1 + 1) \neq 0$, it follows that $y_1 = E_3$. We have already seen that for all $u_1 \in \mathbb{Z}_4$, the output tuple (E_3, E_3, u_1) is connected to all input symbols. The proof is similar for other three cases i.e. when (y_1, y_2, u_1) is connected to 0 and 3, when (y_1, y_2, u_1) is connected to 2 and 1, and when (y_1, y_2, u_1) is connected to 2 and 3.

Next we find all output tuples which are connected to both 0 and 2 but are not connected to 1 or 3. Let (y_1, y_2, u_1) be an output tuple such that $W^+(y_1, y_2, u_1|0) \neq 0$, $W^+(y_1, y_2, u_1|2) \neq 0$, $W^+(y_1, y_2, u_1|1) = 0$ and $W^+(y_1, y_2, u_1|3) = 0$.

First assume $u_1 \in \{0, 2\}$. Since $W(y_2|0) \neq 0$ and $W(y_2|2) \neq 0$, it follows that $y_2 \in \{E_1, E_3\}$ and since $W(y_1|u_1) \neq 0$ and $W(y_1|u_1 + 2) \neq 0$, it follows that $y_1 \in \{E_1, E_3\}$. Note that for $y_1 = E_3$ and $y_2 = E_3$, the output tuple is connected to all inputs and therefore all possible cases are $y_1 = E_1, y_2 = E_1$, $y_1 = E_1, y_2 = E_3$ and $y_1 = E_3, y_2 = E_1$. In all cases it can be shown that $W^+(y_1, y_2, u_1|1) = 0$ and $W^+(y_1, y_2, u_1|3) = 0$. Hence for $u_1 \in \{0, 2\}$, (E_1, E_1, u_1) is connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon^2$ and is not connected to 1 or 3. (E_1, E_3, u_1) is connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 1 or 3. (E_3, E_1, u_1) is connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 1 or 3.

Now assume $u_1 \in \{1, 3\}$. Same as above we have $y_2 \in \{E_1, E_3\}$ and since $W(y_1|u_1) \neq 0$ and $W(y_1|u_1 + 2) \neq 0$, it follows that $y_1 \in \{E_2, E_3\}$. In this case, all possible cases are $y_1 = E_2, y_2 = E_1$, $y_1 = E_2, y_2 = E_3$ and $y_1 = E_3, y_2 = E_1$. In all cases it can be shown that $W^+(y_1, y_2, u_1|1) = 0$ and $W^+(y_1, y_2, u_1|3) = 0$. Hence for $u_1 \in \{1, 3\}$, (E_2, E_1, u_1) is connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon^2$ and is not connected to 1 or 3. (E_2, E_3, u_1) is connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 1 or 3. (E_3, E_1, u_1) is connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 1 or 3.

Therefore, there are four equivalent outputs connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon^2$ and not connected to 1 or 3 and there are eight equivalent outputs connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon\lambda$ and not connected to 1 or 3. Since all of these outputs are equivalent, we can combine them into one output

connected to 0 and 2 with probabilities

$$4 \left(\frac{1}{4} \epsilon^2 \right) + 8 \left(\frac{1}{4} \epsilon \lambda \right) = \epsilon^2 + 2\epsilon\lambda$$

Now we find all output tuples which are connected to both 1 and 3 but are not connected to 0 or 2. Let (y_1, y_2, u_1) be an output tuple such that $W^+(y_1, y_2, u_1|1) \neq 0$, $W^+(y_1, y_2, u_1|3) \neq 0$, $W^+(y_1, y_2, u_1|0) = 0$ and $W^+(y_1, y_2, u_1|2) = 0$.

First assume $u_1 \in \{0, 2\}$. Since $W(y_2|1) \neq 0$ and $W(y_2|3) \neq 0$, it follows that $y_2 \in \{E_2, E_3\}$ and since $W(y_1|u_1 + 1) \neq 0$ and $W(y_1|u_1 + 3) \neq 0$, it follows that $y_1 \in \{E_2, E_3\}$. Note that for $y_1 = E_3$ and $y_3 = E_3$, the output tuple is connected to all inputs and therefore all possible cases are $y_1 = E_2, y_2 = E_2$, $y_1 = E_2, y_2 = E_3$ and $y_1 = E_3, y_2 = E_2$. In all cases it can be shown that $W^+(y_1, y_2, u_1|0) = 0$ and $W^+(y_1, y_2, u_1|2) = 0$. Hence for $u_1 \in \{0, 2\}$, (E_2, E_2, u_1) is connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon^2$ and is not connected to 0 or 2. (E_2, E_3, u_1) is connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 0 or 2. (E_3, E_2, u_1) is connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 0 or 2.

Now assume $u_1 \in \{1, 3\}$. Same as above we have $y_2 \in \{E_2, E_3\}$ and since $W(y_1|u_1 + 1) \neq 0$ and $W(y_1|u_1 + 3) \neq 0$, it follows that $y_1 \in \{E_1, E_3\}$. In this case, all possible cases are $y_1 = E_1, y_2 = E_2$, $y_1 = E_1, y_2 = E_3$ and $y_1 = E_3, y_2 = E_2$. In all cases it can be shown that $W^+(y_1, y_2, u_1|0) = 0$ and $W^+(y_1, y_2, u_1|2) = 0$. Hence for $u_1 \in \{1, 3\}$, (E_1, E_2, u_1) is connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon^2$ and is not connected to 0 or 2. (E_1, E_3, u_1) is connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 0 or 2. (E_3, E_2, u_1) is connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 0 or 2.

Therefore, there are four equivalent outputs connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon^2$ and not connected to 0 or 2 and there are eight equivalent outputs connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon\lambda$ and not connected to 0 or 2. Same as above, since all of these outputs are equivalent, we can combine them into one output connected to 1 and 3 with probabilities $\epsilon^2 + 2\epsilon\lambda$.

We have shown that there is (equivalently) one channel output (call it E_3^+) connected to all inputs $u_2 \in \mathbb{Z}_4$ with conditional probability $\lambda_1 = \lambda^2$ and we have shown that if a channel output is connected to more than one input but is not connected to all inputs, it is either connected to $\{0, 2\}$ and is not connected to $\{1, 3\}$ (call it E_1^+) or it is connected to $\{0, 2\}$ and is not connected to $\{1, 3\}$ (call it E_2^+). 0 and 2 are connected to E_1^+ with probabilities $\epsilon_1 = \epsilon^2 + 2\epsilon\lambda$ and 1 and 3 are connected to E_2^+ with probabilities $\epsilon_1 = \epsilon^2 + 2\epsilon\lambda$. Then for each input $u_2 \in \mathbb{Z}_4$ there exist several outputs which are only connected to u_2

and not other inputs and whose sum of probabilities add up to $1 - \epsilon_1 - \lambda_1$. This completes the proof for W^+ .

2) *Recursion for W^-* : We show that W^- (corresponding to $b_1 = 0$) is equivalent to a channel of the same type as W but with different parameters ϵ_1 and λ_1 corresponding to ϵ and λ respectively; where,

$$\epsilon_1 = 2\epsilon - (\epsilon^2 + 2\epsilon\lambda)$$

$$\lambda_1 = 2\lambda - \lambda_1^2$$

Note that each channel output is a pair $(y_1, y_2) \in \{0, 1, 2, 3, E_1, E_2, E_3\}^2$. The channel W^- can be shown to be as following:

Output pairs $(0, 0)$, $(1, 1)$, $(2, 2)$, $(3, 3)$ are only connected to input 0 each with conditional probability $\frac{1}{4}(1 - \epsilon - \lambda)^2$. This is equivalent to one channel output only connected to 0 with probability $(1 - \epsilon - \lambda)^2$. Output pairs $(0, 2)$, $(1, 3)$, $(2, 0)$, $(3, 1)$ are only connected to input 2 each with conditional probability $\frac{1}{4}(1 - \epsilon - \lambda)^2$. This is equivalent to one channel output only connected to 2 with probability $(1 - \epsilon - \lambda)^2$. Output pairs $(0, 3)$, $(1, 0)$, $(2, 1)$, $(3, 2)$ are only connected to input 1 each with conditional probability $\frac{1}{4}(1 - \epsilon - \lambda)^2$. This is equivalent to one channel output only connected to 1 with probability $(1 - \epsilon - \lambda)^2$. Output pairs $(0, 1)$, $(1, 2)$, $(2, 3)$, $(3, 0)$ are only connected to input 3 each with conditional probability $\frac{1}{4}(1 - \epsilon - \lambda)^2$. This is equivalent to one channel output only connected to 3 with probability $(1 - \epsilon - \lambda)^2$. Output pairs $(0, E_1)$, $(1, E_2)$, $(2, E_1)$, $(3, E_2)$, $(E_1, 0)$, $(E_1, 2)$, $(E_2, 1)$, $(E_2, 3)$ are only connected to inputs 0 and 2 each with conditional probability $\frac{1}{4}\epsilon(1 - \epsilon - \lambda)$. Output pairs (E_1, E_1) , (E_2, E_2) are only connected to inputs 0 and 2 each with conditional probability $\frac{1}{2}\epsilon^2$. This is equivalent to one channel output only connected to 0 and 2 with probability

$$\begin{aligned} \epsilon_1 &= 8 \times \frac{1}{4}\epsilon(1 - \epsilon - \lambda) + 2 \times \frac{1}{2}\epsilon^2 \\ &= 2\epsilon - (\epsilon^2 + 2\epsilon\lambda) \end{aligned}$$

Output pairs $(0, E_2)$, $(1, E_1)$, $(2, E_2)$, $(3, E_1)$, $(E_1, 1)$, $(E_1, 3)$, $(E_2, 0)$, $(E_2, 2)$ are only connected to inputs 1 and 3 each with conditional probability $\frac{1}{4}\epsilon(1 - \epsilon - \lambda)$. Output pairs (E_1, E_2) , (E_2, E_1) are only connected to inputs 1 and 3 each with conditional probability $\frac{1}{2}\epsilon^2$. This is equivalent to one channel output only connected to 1 and 3 with probability $2\epsilon - (\epsilon^2 + 2\epsilon\lambda)$.

Output pairs $(0, E_3)$, $(1, E_3)$, $(2, E_3)$, $(3, E_3)$, $(E_3, 0)$, $(E_3, 1)$, $(E_3, 2)$, $(E_3, 3)$ are connected to all inputs each with conditional probability $\frac{1}{4}\lambda(1 - \epsilon - \lambda)$. Output pairs (E_1, E_3) , (E_2, E_3) , (E_3, E_1) , (E_3, E_2) are connected to all inputs each with conditional probability $\frac{1}{2}\epsilon\lambda$. Output pair (E_3, E_3) is connected to all inputs with conditional probability λ^2 . This is equivalent to one channel output only connected to all

inputs with probability

$$\begin{aligned}\epsilon_1 &= 8 \times \frac{1}{4} \lambda (1 - \epsilon - \lambda) + 4 \times \frac{1}{2} \epsilon \lambda + \lambda^2 \\ &= 2\lambda - \lambda^2\end{aligned}$$

We have listed all 49 channel outputs and the corresponding probabilities. This completes the proof for W^- .

C. Upper Bound on $Z(\bar{W})$

Assume $Z_{d'}(W) < \epsilon$. This implies

$$\frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} \sqrt{W(y|x)W(y|x + \tilde{d})} < \epsilon$$

for all $\tilde{d} \in H \setminus M$. Therefore for each $x \in \mathbf{G}$,

$$\sum_{y \in \mathcal{Y}} \sqrt{W(y|x)W(y|x + \tilde{d})} < q\epsilon \quad (20)$$

The Bhattacharyya parameter of the channel \bar{W} is given by:

$$\begin{aligned}Z(\bar{W}) &= \frac{1}{\bar{q}(\bar{q} - 1)} \sum_{\substack{t_M, t'_M \in T_M \\ t_M \neq t'_M}} \sum_{y \in \mathcal{Y}} \sqrt{\bar{W}(y|t_H + t_M + M) \bar{W}(y|t_H + t'_M + M)} \\ &= \frac{1}{\bar{q}(\bar{q} - 1)} \frac{1}{|M|} \sum_{\substack{t_M, t'_M \in T_M \\ t_M \neq t'_M}} \sum_{y \in \mathcal{Y}} \sqrt{\left(\sum_{m \in M} W(y|t_H + t_M + m) \right) \left(\sum_{m' \in M} W(y|t_H + t'_M + m') \right)} \\ &= \frac{1}{\bar{q}(\bar{q} - 1)} \frac{1}{|M|} \sum_{\substack{t_M, t'_M \in T_M \\ t_M \neq t'_M}} \sum_{y \in \mathcal{Y}} \sqrt{\sum_{m, m' \in M} W(y|t_H + t_M + m) W(y|t_H + t'_M + m')} \\ &\leq \frac{1}{\bar{q}(\bar{q} - 1)} \frac{1}{|M|} \sum_{\substack{t_M, t'_M \in T_M \\ t_M \neq t'_M}} \sum_{y \in \mathcal{Y}} \sum_{m, m' \in M} \sqrt{W(y|t_H + t_M + m) W(y|t_H + t'_M + m')}\end{aligned}$$

Let $x = t_H + t_M + m$ and $x' = t_H + t'_M + m'$. Note that $x - x' = t_M - t'_M + m - m' \in H$ since $t_M, t'_M, m, m' \in H$. Also note that since $t_M \neq t'_M$ and $m - m' \in M$, it follows that $x - x' \notin M$. Now

we use (20) to conclude:

$$\begin{aligned} Z(\bar{W}) &\leq \frac{1}{\bar{q}(\bar{q}-1)} \frac{1}{|M|} \sum_{\substack{t_M, t'_M \in T_M \\ t_M \neq t'_M}} \sum_{m, m' \in M} q\epsilon \\ &\leq \frac{1}{\bar{q}(\bar{q}-1)} \frac{1}{|M|} \left(\frac{|H|}{|M|}\right)^2 |M|^2 q\epsilon = \frac{|M| \cdot |H| \cdot |G|}{|H| - |M|} \epsilon \end{aligned}$$

Remark A.1. For an arbitrary Abelian group \mathbf{G} , let $H \leq \mathbf{G}$ be an arbitrary subgroup and let M be any maximal subgroup of H . If for all $\tilde{d} \in H \setminus M$, $Z_{\tilde{d}}(W) < \epsilon$ then with a similar argument as above we can show that $Z(\bar{W}) < O(\epsilon)$ where \bar{W} is defined by (11).

D. Lower Bound on $Z_{d'+t_H+M}(\bar{W})$

Assume $Z_{d'}(W) > 1 - \epsilon$. Define

$$D_{d'}(W) = \frac{1}{2q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} |W(y|x) - W(y|x + d')|$$

First we show that $Z_{d'}(W) > 1 - \epsilon$ implies $D_{d'}(W) < O(\epsilon)$. Define the following quantities:

$$\begin{aligned} q_{x,y} &= \frac{W(y|x) + W(y|x + d')}{2} \\ \delta_{x,y} &= \frac{1}{2} |W(y|x) - W(y|x + d')| \end{aligned}$$

Then we have

$$\begin{aligned} Z_{d'}(W) &= \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} \sqrt{(q_{x,y} - \delta_{x,y})(q_{x,y} + \delta_{x,y})} \\ &= \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} \sqrt{q_{x,y}^2 - \delta_{x,y}^2} \end{aligned}$$

Also we have

$$D \triangleq \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} \delta_{x,y} = D_{d'}(W),$$

and

$$0 \leq \delta_{x,y} \leq q_{x,y}$$

Note that

$$Z_{d'}(W) \leq \max_{d_{x,y} : \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} d_{x,y} = D} \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} \sqrt{q_{x,y}^2 - d_{x,y}^2}$$

The Lagrangian for this optimization problem is given by

$$\mathcal{L} = \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} \sqrt{q_{x,y}^2 - d_{x,y}^2} - \lambda \left(\frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} d_{x,y} - D \right)$$

we have

$$\frac{\partial}{\partial d_{x,y}} \mathcal{L} = -\frac{d_{x,y}}{\sqrt{q_{x,y}^2 - d_{x,y}^2}} - \frac{\lambda}{q}$$

and

$$\frac{\partial^2}{\partial d_{x,y}^2} \mathcal{L} = -\frac{q_{x,y}^2}{(q_{x,y}^2 - d_{x,y}^2)^{\frac{3}{2}}} \leq 0$$

Define $\gamma = -\frac{\lambda}{q}$ to get $d_{x,y} = \sqrt{\frac{\gamma^2}{1+\gamma^2} q_{x,y}}$. We have $\sum_{y \in \mathcal{Y}} q_{x,y} = 1$, therefore,

$$\begin{aligned} \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} d_{x,y} &= \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} \sqrt{\frac{\gamma^2}{1+\gamma^2} q_{x,y}} \\ &= \sqrt{\frac{\gamma^2}{1+\gamma^2}} \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} q_{x,y} \\ &= \sqrt{\frac{\gamma^2}{1+\gamma^2}} \end{aligned}$$

Therefore we have $D = \sqrt{\frac{\gamma^2}{1+\gamma^2}}$ and hence $d_{x,y} = D q_{x,y}$. For this choice of $d_{x,y}$ we have

$$\begin{aligned} \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} \sqrt{q_{x,y}^2 - d_{x,y}^2} &= \frac{\sqrt{1-D^2}}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} q_{x,y} \\ &= \sqrt{1-D^2} \end{aligned}$$

Therefore, we have shown that $Z_{d'}(W) \leq \sqrt{1-D_{d'}(W)^2}$. This implies that $D_{d'}(W) < 2\epsilon - \epsilon^2 = O(\epsilon)$.

Next, we show that $D_{d'}(W) < \epsilon$ implies $Z_{d'}(W) > 1 - O(\epsilon)$. We need the following lemma:

Lemma A.1. *For constants $0 \leq a \leq b \leq 1$, with $b - a \leq \delta$,*

$$\sqrt{ab} \geq \frac{a+b}{2} - \frac{\delta}{2}$$

Proof: Note that

$$\frac{a+b}{2} - \sqrt{ab} \leq \max_{0 \leq x-a \leq \delta} \frac{a+x}{2} - \sqrt{ax}$$

We have

$$\frac{\partial}{\partial x} \left[\frac{a+x}{2} - \sqrt{ax} \right] = \frac{1}{2} - \frac{a}{2\sqrt{ax}} \geq 0$$

for all $x \geq a$. Therefore the maximum is attained at $x = a + \delta$. Therefore,

$$\frac{a+b}{2} - \sqrt{ab} \leq \frac{a+(a+\delta)}{2} - \sqrt{a(a+\delta)}$$

The maximum of the right hand side is attained at $a = 0$, hence,

$$\frac{a+b}{2} - \sqrt{ab} \leq \frac{\delta}{2}$$

■

Assume $D_{d'}(W) < \epsilon$. We have

$$\begin{aligned} 1 - Z_{d'}(W) &= 1 - \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} \sqrt{W(y|x)W(y|x+d')} \\ &= \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} \left(\frac{W(y|x) + W(y|x+d')}{2} - \sqrt{W(y|x)W(y|x+d')} \right) \\ &\stackrel{(a)}{\leq} \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathcal{Y}} \frac{1}{2} |W(y|x) - W(y|x+d')| \\ &= D_{d'}(W) \end{aligned}$$

where (a) follows from Lemma A.1 with $a = W(y|x)$, $b = W(y|x+d')$ and $\delta = |W(y|x) - W(y|x+d')|$.

This shows that $D_{d'}(W) < \epsilon$ implies $Z_{d'}(W) > 1 - \epsilon$.

Next, we show that $D_{d'}(W) < \epsilon$ implies $D_{d'+t_H+M}(\bar{W}) < O(\epsilon)$. We have

$$\begin{aligned} D_{d'+t_H+M}(\bar{W}) &= \frac{1}{2q} \sum_{t_M \in T_M} \sum_{y \in \mathcal{Y}} |\bar{W}(y|t_H+t_M+M) - \bar{W}(y|t_H+t_M+d'+M)| \\ &= \frac{1}{\bar{q}} \frac{1}{|M|} \sum_{t_M \in T_M} \sum_{y \in \mathcal{Y}} \left| \sum_{m \in M} W(y|t_H+t_M+m) - \sum_{m \in M} W(y|t_H+t_M+d'+m) \right| \\ &\leq \frac{1}{\bar{q}} \frac{1}{|M|} \sum_{t_M \in T_M} \sum_{y \in \mathcal{Y}} \sum_{m \in M} |W(y|t_H+t_M+m) - W(y|t_H+t_M+d'+m)| \\ &\leq \frac{1}{\bar{q}} \frac{1}{|M|} 2q D_{d'}(W) \end{aligned}$$

This shows that $D_{d'}(W) < \epsilon$ implies $D_{d'+t_H+M}(\bar{W}) < \frac{2q\epsilon}{\bar{q}|M|} = O(\epsilon)$.

We have shown that $Z_{d'}(W) > 1 - \epsilon$ implies $D_{d'}(W) < 2\epsilon - \epsilon^2 = O(\epsilon)$. This implies $D_{d'+t_H+M}(\bar{W}) < \frac{2q(2\epsilon-\epsilon^2)}{\bar{q}|M|} = O(\epsilon)$ and this in turn implies $Z_{d'+t_H+M}(\bar{W}) > 1 - \frac{2q(2\epsilon-\epsilon^2)}{\bar{q}|M|} = 1 - O(\epsilon)$.

Remark A.2. For an arbitrary Abelian group \mathbf{G} , let $H \leq \mathbf{G}$ be an arbitrary subgroup and let M be any maximal subgroup of H . If for some $\tilde{d} \in H \setminus M$, $Z_{\tilde{d}}(W) > 1 - \epsilon$ then with a similar argument as above, we can show that $Z_{\tilde{d}+t_H+M}(\bar{W}) > 1 - O(\epsilon)$ where \bar{W} is defined by (11).

E. Alternate Proof for a Lower Bound on $Z_{d'+t_H+M}(\bar{W})$

In Appendix D, we proved that $Z_{d'}(W) > 1 - \epsilon$ implies $Z_{d'+t_H+M}(\bar{W}) > 1 - O(\epsilon)$. In this part, we give an alternate proof of this statement for the \mathbb{Z}_{p^r} case.

Assume $Z_{d'}(W) > 1 - \epsilon$. It follows that

$$\sum_{x \in \mathbf{G}} \left[1 - \sum_{y \in \mathcal{Y}} \sqrt{W(y|x)W(y|x+d')} \right] < q\epsilon$$

Similar to the previous case, we have for all $x \in \mathbf{G}$,

$$\sqrt{1 - Z(W_{\{x, x+2d'\}})} \leq 2\sqrt{q\epsilon}$$

Repeated application of the above lemma yields $\forall x, x' \in \mathbf{G} : x - x' \in \langle d' \rangle$,

$$\sqrt{1 - Z(W_{\{x, x'\}})} \leq q\sqrt{q\epsilon} \quad (21)$$

We have

$$\begin{aligned} Z_{d'+t_H+M}(\bar{W}) &= \frac{1}{\bar{q}} \sum_{t_M \in T_M} \sum_{y \in \mathcal{Y}} \sqrt{\bar{W}(y|t_H + t_M + M) \bar{W}(y|t_H + t_M + d' + M)} \\ &= \frac{1}{\bar{q}} \sum_{t_M \in T_M} \sum_{y \in \mathcal{Y}} \sqrt{\sum_{m, m' \in M} \frac{1}{|M|^2} W(y|t_H + t_M + m) W(y|t_H + t_M + d' + m')} \\ &\stackrel{(a)}{\geq} \frac{1}{\bar{q}} \sum_{t_M \in T_M} \sum_{y \in \mathcal{Y}} \sum_{m, m' \in M} \frac{1}{|M|^2} \sqrt{W(y|t_H + t_M + m) W(y|t_H + t_M + d' + m')} \\ &\geq \frac{1}{\bar{q}} \sum_{t_M \in T_M} \min_{m, m' \in M} \sum_{y \in \mathcal{Y}} \sqrt{W(y|t_H + t_M + m) W(y|t_H + t_M + d' + m')} \end{aligned}$$

where (a) follows since $\sqrt{\cdot}$ is a concave function. Let $x = t_H + t_M + m$ and $x' = t_H + t_M + d' + m'$. It follows that $x' - x = d' + (m' - m)$. Since $d', m', m \in H$ we have $x' - x \in H$. Since \mathbf{G} and hence H are \mathbb{Z}_{p^r} rings it follows that $d' \in H \setminus M$ generates H ; hence $x' - x \in \langle d' \rangle$. We can use (21) to get

$$Z_{d'+t_H+M}(\bar{W}) \geq \frac{1}{\bar{q}} \sum_{t_M \in T_M} \min_{m, m' \in M} (1 - q^3\epsilon) = 1 - \frac{q^3\epsilon}{\bar{q}}$$

It follows that $Z_{d'+t_H+M}(\bar{W}) > 1 - O(\epsilon)$.

F. The Rate of Polarization

Recall that for $t = 0, \dots, r$, $(Z^t)^{(n)} = \sum_{d \notin H_t} Z_d(W_N^{(J_n)})$ where J_n is uniform over $\{1, 2, \dots, 2^n\}$. For $t = 0, \dots, r$, define $(Z_{\max}^t)^{(n)} = \max_{d \notin H_t} Z_d(W_N^{(J_n)})$ where J_n is same as above. Since for all $d \in \mathbf{G}$, $Z_d(W^+) = Z_d(W)^2$ it follows that $Z_{\max}^t(W^+) \leq Z_{\max}^t(W)^2$. It has been shown in [2, p. 6] that

$$Z_d(W^-) \leq 2Z_d(W) + \sum_{\substack{\Delta \neq 0 \\ \Delta \neq -d}} Z_{\Delta}(W) Z_{d+\Delta}(W)$$

Note that for any $\Delta \in G$, $d \notin H_t$ implies that either $\Delta \notin H_t$ or $d + \Delta \notin H_t$. Therefore, $d \notin H_t$ implies either $Z_{\Delta}(W) \leq Z_{\max}^t(W)$ or $Z_{d+\Delta}(W) \leq Z_{\max}^t(W)$ (or both). Since $Z_{\Delta}(W)$ and $Z_{d+\Delta}(W)$ both take values from $[0, 1]$, it follows that

$$Z_{\Delta}(W) Z_{d+\Delta}(W) \leq Z_{\max}^t(W)$$

Therefore, for any $d \notin H_t$, $Z_d(W^-) \leq 2Z_d(W) + qZ_{\max}^t(W)$. Hence

$$\begin{aligned} Z_{\max}^t(W^-) &= \max_{d \notin H_t} Z_d(W^-) \\ &\leq \max_{d \notin H_t} (2Z_d(W) + qZ_{\max}^t(W)) \\ &\leq (q+2)Z_{\max}^t(W) \end{aligned}$$

Since for all d Z_d^n converges to a Bernoulli random variable it follows that $(Z_{\max}^t)^{(n)}$ also converges to a $\{0, 1\}$ -valued random variable $(Z_{\max}^t)^{(\infty)}$. Note that $P((Z_{\max}^t)^{(\infty)} = 0) = P((Z^t)^{\infty} = 0) = \sum_{s=t}^r p_s$. Therefore, $(Z_{\max}^t)^{(n)}$ satisfies the conditions of [11, Theorem 1] and hence

$$\lim_{n \rightarrow \infty} P\left((Z_{\max}^t)^{(n)} < 2^{-2^{\beta n}}\right) = P\left((Z_{\max}^t)^{(\infty)} = 0\right)$$

for any $\beta < \frac{1}{2}$. It clearly follows that $\lim_{n \rightarrow \infty} P\left(q(Z_{\max}^t)^{(n)} < 2^{-2^{\beta n}}\right) = P\left((Z_{\max}^t)^{(\infty)} = 0\right)$. Note that the event $\{(Z^t)^{(n)} < 2^{-2^{\beta n}}\}$ includes the event $\{q(Z_{\max}^t)^{(n)} < 2^{-2^{\beta n}}\}$. Therefore,

$$\lim_{n \rightarrow \infty} P\left((Z^t)^{(n)} < 2^{-2^{\beta n}}\right) \geq P\left((Z^t)^{\infty} = 0\right)$$

Similarly, for an arbitrary Abelian group \mathbf{G} and a subgroup H of \mathbf{G} , define $(Z_{\max}^H)^{(n)} = \max_{d \notin H} Z_d(W_N^{(J_n)})$ where J_n is defined as above. It is straightforward to show that $(Z_{\max}^H)^{(n)}$ satisfies the conditions of [11, Theorem 1]. Therefore, with an argument similar to above, we can show that,

$$\lim_{n \rightarrow \infty} P\left((Z^H)^{(n)} < 2^{-2^{\beta n}}\right) \geq P\left((Z^H)^{\infty} = 0\right)$$

for any $\beta < \frac{1}{2}$.

REFERENCES

- [1] E. Arikan, "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.
- [2] E. Sasoglu, E. Telatar, and E. Arikan, "Polarization for arbitrary discrete memoryless channels," *IEEE Information Theory Workshop*, Dec. 2009, Lausanne, Switzerland.
- [3] R. Mori and T. Tanaka, "Channel Polarization on q -ary Discrete Memoryless Channels by Arbitrary Kernels," *Proc. IEEE Int. Symp. Information Theory*, 2010, Austin, TX.
- [4] E. Abbe and E. Telatar, "Polar Codes for the m -User MAC," 2010, Online: <http://arxiv.org/abs/1002.0777>.
- [5] W. Park and A. Barg, "Polar codes for q -ary channels, $q = 2^r$," 2012, Online: <http://arxiv.org/abs/1107.4965>.
- [6] A. G. Sahebi and S. S. Pradhan, "Multilevel Polarization of Polar Codes Over Arbitrary Discrete Memoryless Channels," *Proc. 49th Allerton Conference on Communication, Control and Computing*, Sept. 2011.
- [7] R. Ahlswede, "Group codes do not achieve Shannons's channel capacity for general discrete channels," *The annals of Mathematical Statistics*, vol. 42, no. 1, pp. 224–240, Feb. 1971.
- [8] A. F. Karr, *Probability*. Springer, 1993.
- [9] N. J. Bloch, *Abstract Algebra With Applications*. Englewood Cliffs, New Jersey: Prentice-Hall, Inc, 1987.
- [10] A. G. Sahebi and S. S. Pradhan, "On the Capacity of Abelian Group Codes Over Discrete Memoryless Channels," *Proc. IEEE Int. Symp. Information Theory*, 2011, Saint Petersburg, Russia.
- [11] E. Arikan and E. Telatar, "On the rate of channel polarization," *Proceedings of IEEE International Symposium on Information Theory*, 2009, Seoul, Korea.